D-Link Airspot
DSA-5100
Enterprise Gateway

Manual

April 2006
v. 1.03

D-Link®

Building Networks for People

Contents

Package Contents

1   **D-Link DSA-5100 Airspot Enterprise Gateway**

2   CD-ROM with manual

3   Quick Installation Guide

4   Three (3) CAT5 UTP/Straight-through (Ethernet) cables

5   One (1) CAT5 UTP/Cross-over cable

6   One (1) Console cable

7   1 PC-Style Power cable to 110 VAC

If any of the above items are missing, please contact your reseller.

System Requirements for Configuration:

■   Computers with Windows, Macintosh, or Linux-based
operating systems with an installed Ethernet adapter

■   Internet Explorer Version 6.0 or Netscape Navigator
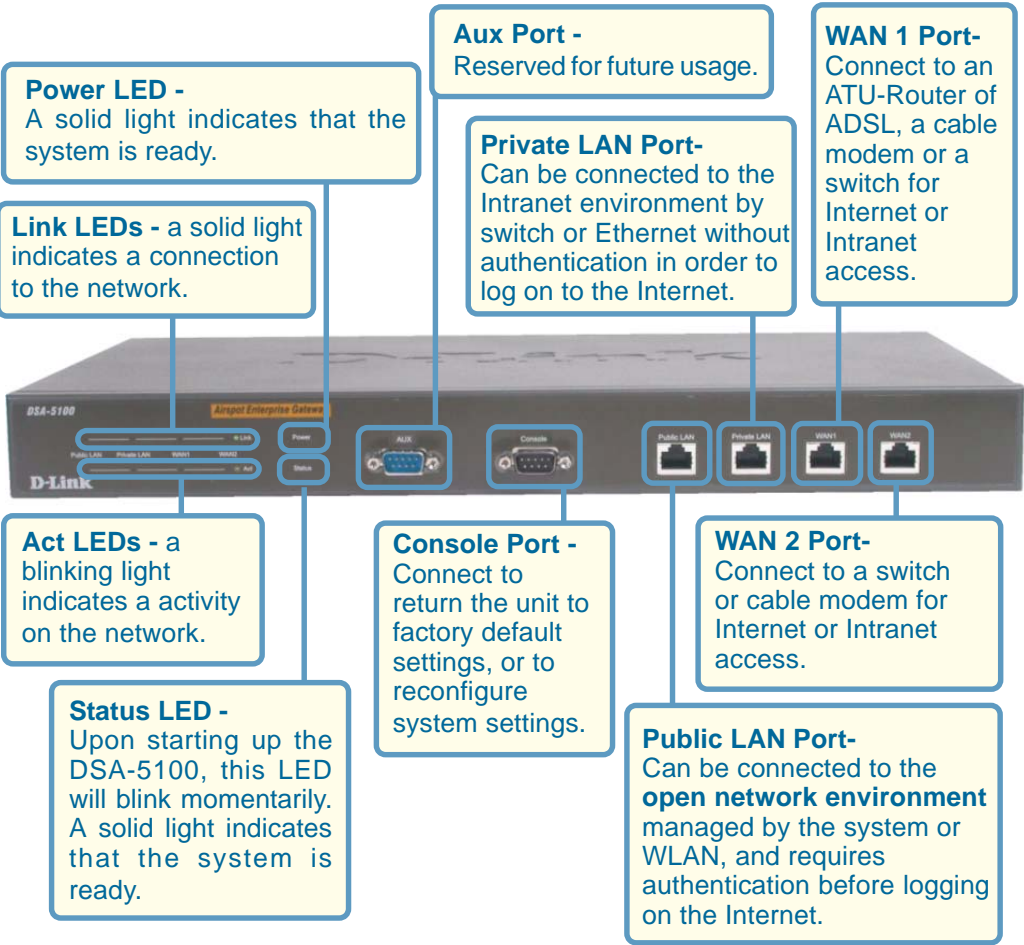Version 6.0 and above

Introduction

The D-Link DSA-5100 Airspot Enterprise Gateway is an advanced network access control system supporting Ethernet, Fast Ethernet or an IEEE 802.11 wireless LAN (WLAN) separately and simultaneously.

The DSA-5100 can be configured with a standard HTML browser (i.e., Internet Explorer, or Netscape Navigator) operating on Windows 98SE/Me/2000/XP, Macintosh OS 9, Macintosh OS X (v10.1.5 or later), Linux, or Pocket PC 2000/2002. The DSA-5100 allows the operator to offer wired or wireless networking services and access to the Internet when used with a switch or wireless access point respectively. The device features many management settings allowing for private and public access to the Internet and the necessary privilege mechanisms to permit this usage.

Front Panel

Aux Port - Reserved for future usage.

WAN 1 Port- Connect to an ATU-Router of ADSL, a cable modem or a switch for Internet or Intranet access.

Power LED - A solid light indicates that the system is ready.

Private LAN Port- Can be connected to the Intranet environment by switch or Ethernet without authentication in order to log on to the Internet.

Link LEDs - a solid light indicates a connection to the network.

Act LEDs - a blinking light indicates a activity on the network.

Console Port - Connect to return the unit to factory default settings, or to reconfigure system settings.

WAN 2 Port- Connect to a switch or cable modem for Internet or Intranet access.

Status LED - Upon starting up the DSA-5100, this LED will blink momentarily. A solid light indicates that the system is ready.

Public LAN Port- Can be connected to the **open network environment** managed by the system or WLAN, and requires authentication before logging on the Internet.

Rear Panel

Connector for **Power Cord.**

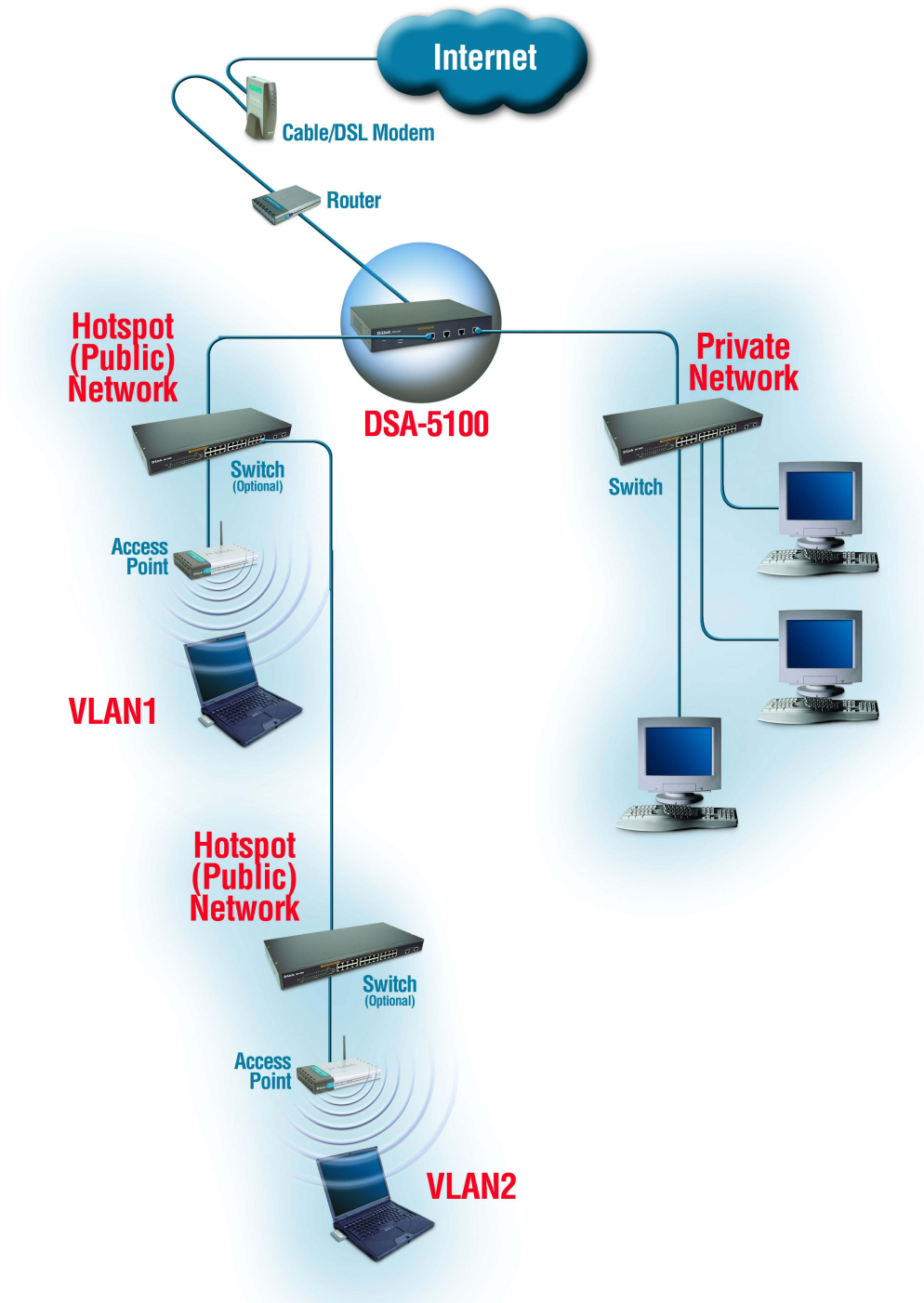**Power Switch-** ON/OFF switch.

Features

- Supports IEEE 802.1x

- Supports IEEE 802.1q VLAN

- Supports IEEE 802.3 ad

- WAN interface supports static IP, DHCP client, and PPPoE client

- WAN2 interface supports static IP

- Supports NAT mode, router mode and bridge mode

- Built-in DHCP server

- Built-in NTP client

- Supports redirect of network data

- Supports IPSec(ESP), PPTP and H.323 pass through (under NAT)

- Customizable static routing table

- Supports virtual server

- Supports DMZ server

- Supports machine operation status monitoring and reporting system

- Supports roaming across networks

- Provides several DoS protection mechanisms

- Customizable packet filter rules

- Customizable walled garden (free surfing area)

- The DSA-5100 supports at least 400 on-line users concurrently

- Supports POP3, RADIUS, and LDAP authentication mechanisms

- Supports two or more authentication mechanisms simultaneously

- Can set the time for the user to logon to the system

- Can set the user's idle time

- Can specify the connection to MAC address without authentication

- Can specify the connection to IP address without authentication

Features (continued)

- Permits or refuses all connections when the WAN interface fails
- Supports Web-based logon
- Provides several friendly logout methods
- Supports RADIUS account roaming
- Provides online status monitoring and history traffic
- Supports SSL encrypted web administration interface and user logon interface
- Customizable user login & logout web interface
- Customizable redirect after users are successfully authenticated during login & logout
- Supports Console management interface
- Supports SSH remote administration interface
- Supports Web-based administration interface
- Supports SNMP v2
- Supports user's bandwidth restriction
- Supports remote firmware upgrade
- Supports built-in user database and RADIUS accounting

A Sample Network Setup

Internet

Cable/DSL Modem

Router

DSA-5100

Hotspot (Public) Network

Switch (Optional)

Access Point

VLAN1

Hotspot (Public) Network

Switch (Optional)

Access Point

VLAN2

Private Network

Switch

Installation Requirements

1. Standard 10/100Base-T, including four network cables with RJ-45 connectors.

2. All PCs need to install the TCP/IP network protocol.

Setting Up the DSA-5100

1.   Make sure the power of the DSA-5100 is turned off.

2.   Connecting the WAN1 and WAN2 ports.
Use one of the supplied straight-through cables to connect the DSA-5100 to the network not managed by the DSA-5100 system (such as and ATU router for ADSL, the Ethernet port of a cable modem, or a switch or hub on a LAN).

3.   Connecting the Public LAN port.
The Public LAN port is used to provide authentication based Internet access for Ethernet (with switch) or WLAN (with AP) clients. Use one of the supplied straight-through Ethernet cables if connecting to a hub or switch. Use the supplied crossover cable if connecting directly to an AP or PC.

Warning: The Public LAN port cannot connect to a Layer 3 device.

4.   Connecting the Private LAN port.
The Private LAN port is used to provide Internet access without authentication for your existing Private Network. Use one of the supplied straight-through Ethernet cables if connecting to a hub or switch. Use the supplied crossover cable if connecting directly to an AP or PC.

5.   Turn on the power.
Plug the bundled power cord connector into the socket and then turn on the power.

6.   Check the LED indicating light.
After the power is ON, the power LED should be lit. The WAN1, WAN2, Public LAN, and Private LAN LEDs will light up with a valid Ethernet connection.

Setting Up the DSA-5100 (continued)

TCP/IP Network Setup

■ For Windows 98SE/ME/2000/XP, you need to keep the default TCP/IP settings ("obtain IP and DNS address automatically") to communicate with the DSA-5100.

■ The DSA-5100 leases DHCP addresses from the Public and Private LAN ports for ease of configuration.

■ For Non-Server Windows operating systems, the default setting for TCP/IP is "DHCP client," which will obtain an IP address automatically.

■ If you wish to use a static IP on the public or private LAN section, or you wish to check the TCP/IP setup, please refer to the Appendix – Windows TCP / IP Setup.

Internet Access Configuration

To configure your PCs to use the DSA-5100 for Internet access, follow this procedure.

For Windows 98SE/2000

■ Please select **Start Menu** - **Control Panel** - **Internet Options**.
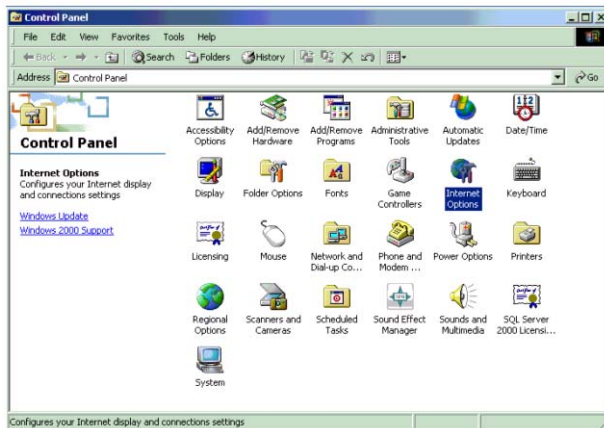
■ Select the Connection tab, and click the **Setup** button.
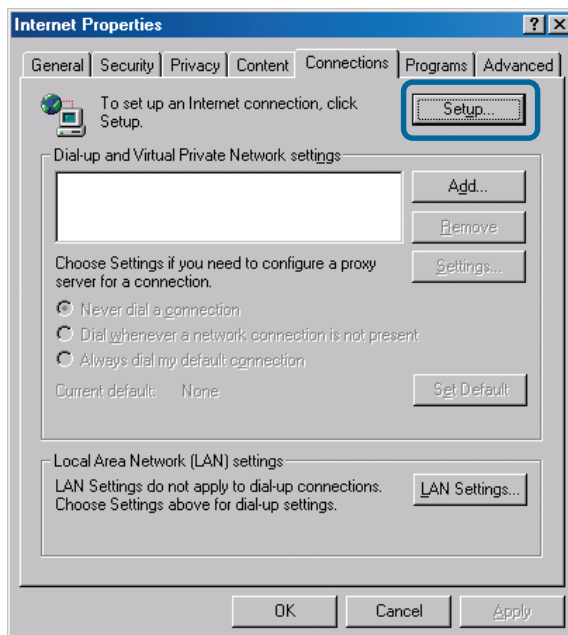
Internet Access Configuration (continued)

■ Select "**I want to set up my Internet connection manually, or I want to connect through a local Area network (LAN)**" and click **Next**.
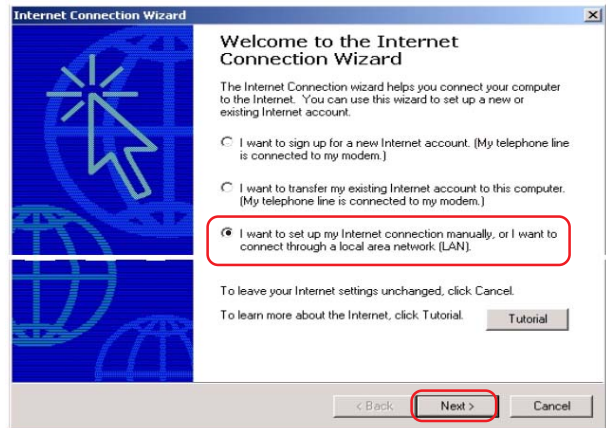
■ Select **"I connect through a local area network (LAN)**" and click **Next**.

■ Ensure all of the boxes on the local area network Internet configuration screen are **unchecked**.

■ Check **No**, when prompted "**Do you want to set up an Internet mail account now?**" Click **Next**.

■ Click **Finish** to close the Internet Connection Wizard. The Internet Connection Setup is now complete.

For Windows XP

■ Select **Start Menu** - **Control Panel** - **Network and Internet Connection**.

■ Select the Connection tab, and click the **Setup** button.

■ Click **Next** on the **New Connection Wizard** screen.

■ Select **Connect to the Internet** and click **Next**.

■ Select **Set up my connection manually** and click **Next**.

■ Check **Connect using a broadband connection that is always on** and click **Next**.

■ Click **Finish** to close the New Connection Wizard. Internet Connection Setup is now complete.

Using the Configuration Utility

To configure the DSA-5100, connect a computer to the Private LAN port of the DSA-5100 with the supplied crossover Ethernet cable.

- ■ First, disable the **Access the Internet using a proxy server** function. To disable this function, go to **Control Panel > Internet Options > Connections > LAN Settings** and uncheck the enable box.

- ■ Start your Microsoft Internet Explorer Web browser program.

- ■ Type the IP address of the DSA-5100 (the default IP address is 192.168.0.40, preceded by https://) in the address field and press Enter. Make sure that the IP addresses of the DSA-5100 and your computer are in the same network.
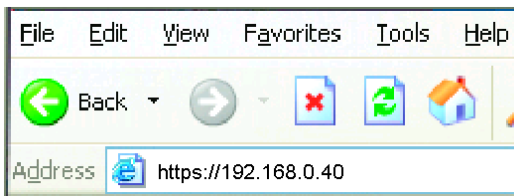
Log-in Screen

*You can log in as **admin** or as **manager**.*

admin -
The administrator of the DSA-5100.

    User Name: admin

    Password: admin

manager -
Access to the manager user account only.

    User Name: manager
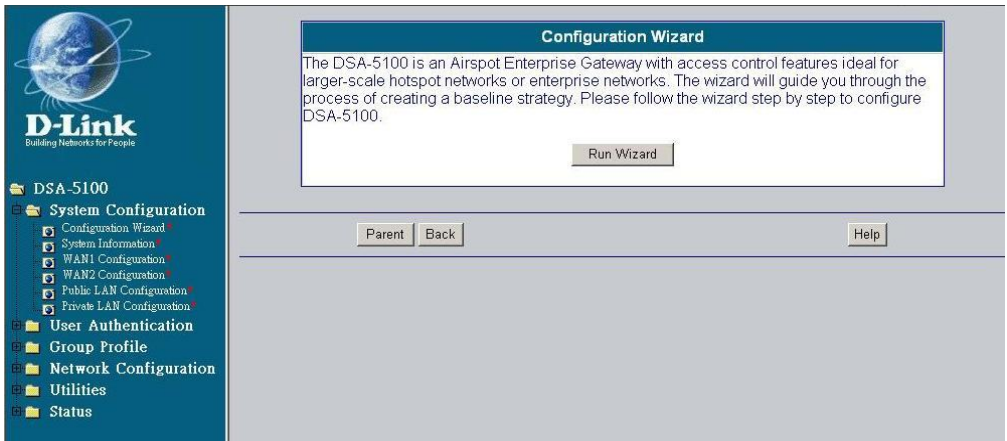
    Password: manager

After you log in, click **Enter**.
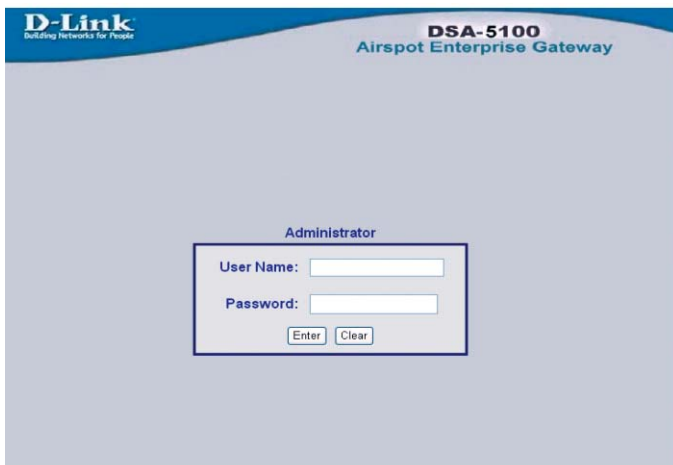
Using the Configuration Utility (continued)

System Configuration > Configuration Wizard
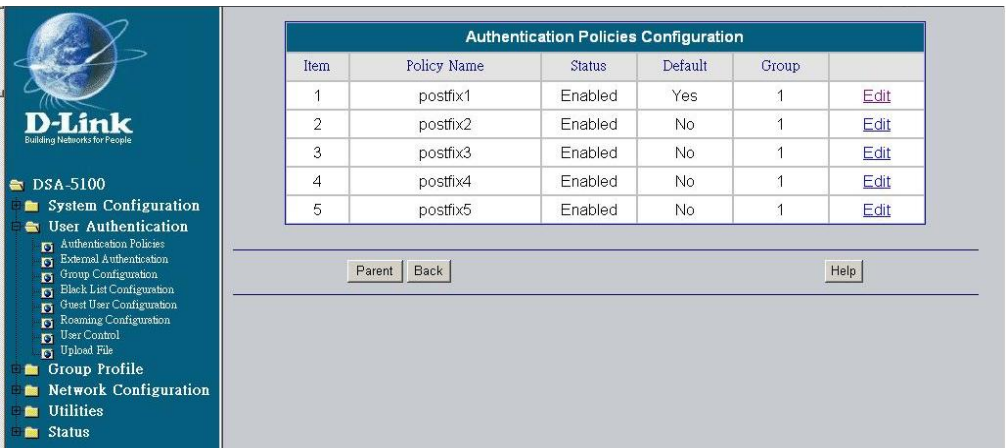
The **System Configuration>Configuration Wizard** screen will appear if you logged in as **admin**. For more information on the **Setup Wizard**, please see the *Installation Guide*, included with your purchase. You can access the configuration features from this window.

User Authentication > Authentication policies

The **User Authentication>Authentication policies** screen will appear if you logged in as a manager. For more information on the **Setup Wizard**, please see the *Installation Guide*. You can access the configuration features from this window.

Using the Configuration Utility (continued)

System Configuration > System Information

System Name: DSA-5100 is the default system name. You may wish to rename it to indicate your company, department, or the service you would like to provide.

Administrator Info: You can edit the System Administrator's information here (e.g., name, phone number, and e-mail).

Succeed Page: Enter a URL which all users will be re-directed to after a successful login. This is typically defined as the home page of the host company, e.g: http://www.dlink.com. No matter which URL a user originally attempts to connect to, he/she will be directed to the URL defined here first.

Remote Management IP: You can allow SSH or HTTPS connections from the WAN for management purposes. Access is limited to a specific IP address or network (e.g., 192.168.2.1 might be used for a specifici IP address. 10.2.3.0/24 for a specific IP Network. **24** indicates the number of bits for the subnet mask).

Access History IP : Specify an IP address to be used by the billing system to connect to the DSA-5100 to get billing history information.

Using the Configuration Utility (continued)

System Configuration > System Information (continued)

SNMP: The DSA-5100 supports SNMP v2 read only data access. The Administrator can specify the IP address and the SNMP community name to determine the target of the management information base (MIB) exported from the DSA-5100.

User Logon SSL: Allows the admin to choose either https (encrypted username/password), or http (non-encrypted username/password) as the login page.

Time: **Enable NTP:** The DSA-5100 supports NTP communication protocol for correct network time. Please specify the IP address or DNS name of an SNTP server on the system configuration interface.

> **Time Zone**: Set up the time zone for the DSA-5100. The default is GMT+08:00. (Taipei)

Set Device Date and Time: Manually specify system time.

Using the Configuration Utility (continued)

System Configuration > WAN1 Configuration > Static IP Mode

WAN1 Configuration

D-Link
Building Networks for People

📁 DSA-5100
📁 System Configuration
  📄 Configuration Wizard
  📄 System Information
  📄 WAN1 Configuration
  📄 WAN2 Configuration
  📄 Public LAN Configuration

WAN1 Port

⦿ Static IP Address
  IP address   10.2.3.88 *
  Subnet mask   255.255.255.0 *
  Default gateway   10.2.3.254 *
  Primary DNS Server   _____ *
  Secondary DNS Server _____
  Bridge Mode   ○ Enable ⦿ Disable
○ Dynamic IP Address
○ PPPoE Client

Static IP Address:

IP address: Enter the IP address provided to you by your ISP (Required).

Subnet mask: Enter the subnet mask provided to you by your ISP. All devices on the network must share the same subnet mask (Required).

Default Gateway: Enter the gateway IP address provided to you by your ISP (Required).

Primary DNS Server: Enter the IP address of the primary DNS server (Required).
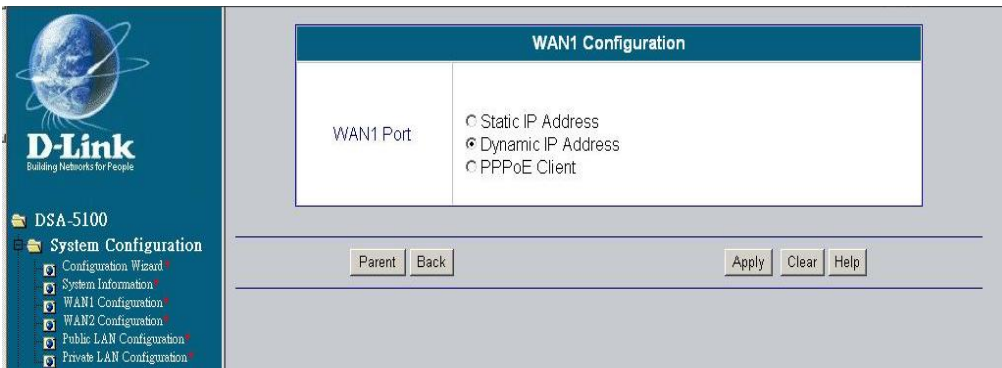
Secondary DNS Server: Enter the IP address of the secondary DNS server (Optional).

Bridge Mode: This device can be configured in Bridge mode. All interfaces bind to the same IP. Only one set of IP addresses can be used for management. The advantage is that there is no need to readjust any network infrastructure, just plug and use. When you click **Enable**, the VLAN function of the Public LAN is disabled.

Note: WAN1 must have a static IP address in order to utilize the 802.3ad WAN link aggregation feature. If you cancel the static IP address, then the option of choice for 802.3ad is also canceled. (Please see the WAN2 configuration that follows for information on configuring 802.3ad.)

Using the Configuration Utility (continued)
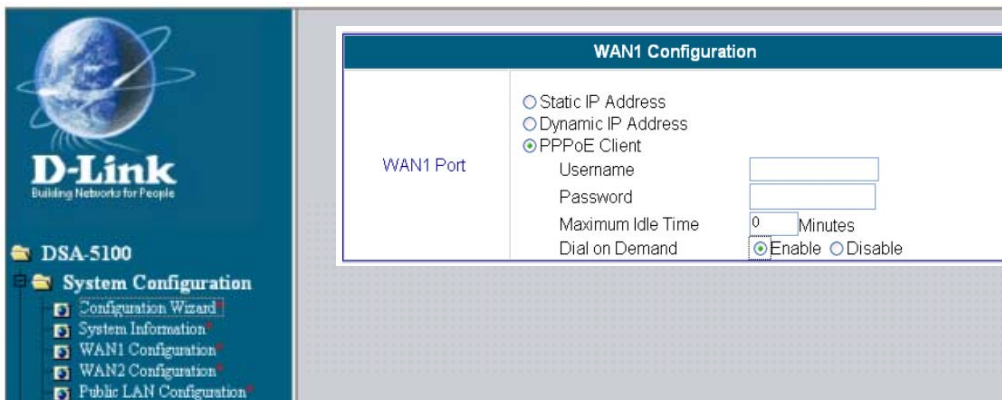
System Configuration > WAN1 > Dynamic IP Address

Select this option if there is a DHCP server on the network or to obtain an IP address automatically from your ISP.

System Configuration > WAN1 > PPPoE

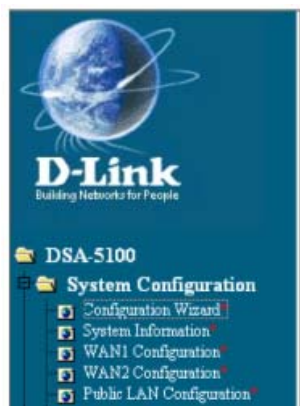

Most DSL users will select this option.

User Name & Password:

Enter the user name and password that is assigned by your ISP.

Maximum Idle Time & Dial on demand:

These fields are optional.

Using the Configuration Utility (continued)

System Configuration > WAN2 > Static IP Address

Static IP Address:

IP address: Enter the IP address provided to you by your ISP.

Subnet mask: Enter the subnet mask provided to you by your ISP. All devices on the network must share the same netmask.

Default Gateway: Enter the IP address of the gateway provided to you by your ISP.

Dynamic IP Address: Choose this option if there is a DHCP server on the unmanaged network.

802.3ad: Set WAN2 to 802.3ad mode only if WAN1 is configured for a static IP. When 802.3ad is enabled, the sum of the bandwidths of WAN1 and WAN2 is used for the total bandwidth (provided that WAN1 and WAN2 are connected to the same switch(es) that also supports 802.3ad.

Using the Configuration Utility (continued)

System Configuration > Public LAN > Global Public LAN Configuration

Global LAN Configuration	
Enable IP PNP	⊙ Enable ○ Disable
Enable Mobile IP	○ Enable ⊙ Disable
Public LAN Configuration	
VLAN	○ Enable ⊙ Disable

You can set the system to start or stop IP PNP or Mobile IP on the Public LAN and Private LAN simultaneously.

> **1. IP PNP:** At the user end, you can use any IP address (with gateway and DNS address) to connect to the Internet; no matter what the IP address at the user end is, you can access the network resources properly and authenticate through the DSA-5100.
> Note: This function can only be activated under NAT.

> **2. Mobile IP:** If you construct a network environment using several DSA-5100s, a user can use the same group of IP configurations. When you roam at different locations, or download data, the connection will not be disconnected.

System Configuration > Public LAN > Public LAN Configuration

If you want to configure multiple Authentication networks on the Public LAN, please select the **Enable VLAN** option on the public LAN interface.

After the **Enable VLAN** option is selected, the following screen will appear. Choose the desired Item and click **Edit** to enter the VLAN interface configuration screen.

Using the Configuration Utility (continued)

Public LAN Configuration			
Public LAN Port	VLAN		◉ Enable ○ Disable
VLAN			
Item	Tag	Status	
VLAN 1	111	Enable	Edit
VLAN 2		Disable	Edit
VLAN 3		Disable	Edit
VLAN 4		Disable	Edit
VLAN 5		Disable	Edit

The system will confirm if you want to Enable VLAN; please click **Enable** to continue.

VLAN Interface Configuration	
VLAN	◉ Enable ○ Disable

After you click **Enable**, the following screen will appear. See the following description for details.

VLAN Interface Configuration	
VLAN 1	◉ Enable ○ Disable
	User Authentication ◉ Enable ○ Disable
	VLAN Tag [ ] *
	Mode [NAT ▼]
	IP Address [ ] *
	Subnet Mask [ ] *
VLAN DHCP Configuration	◉ Disable DHCP Server
	○ Enable DHCP Server
	○ DHCP Relay

Enable/Disable: Enable or Disable the functions of VLAN.

User Authentication: Control the User Authentication method or policy according to individual VLAN.(default is Disabled).

Using the Configuration Utility (continued)

VLAN Tag: Please enter any numbers from 0~4000 as a Tag for each VLAN. (These VLAN IDs must match the managed switch.)

Specific Route Profile: Select your desired Specific Route Profile rules from the pull-down menu, or choose **None**. (It will appear after disabling the User Authentication option.)

Mode: **NAT Mode:** All IP addresses externally connected through the VLAN Port (these IP addresses must belong to the same network as the VLAN Port) will be converted into the IP address of the WAN1 Port by the DSA-5100 and connected to the outside.

Router Mode: All IP addresses externally connected through the VLAN Port use their own IP address for external connections. In this case, the DSA-5100 functions as a router.

IP Address: Enter the desired IP address for the VLAN Interface.

Subnet Mask: Enter the desired Subnet Mask for the VLAN Interface.

Public LAN > VLAN > DHCP Configuration

Disable DHCP Server: Choose this option if you do not wish to use the built-in DHCP Server feature in the DSA-5100.

Enable DHCP Server: Selecting this option activates the device's built-in DHCP server. Configure the DHCP server with the following properties:

Using the Configuration Utility (continued)

Public LAN > VLAN > DHCP Configuration (continued)

Enable DHCP Server (continued):

DHCP Scope

Start IP Address: Enter the starting IP address of the pool, from which the DHCP server will assign to the DHCP-enabled devices (clients) on the network.

End IP Address: Enter the last IP address in the sequence of addresses from which the DHCP server will assign addresses.

Primary DNS Server: Enter the IP address of the preferred DNS server.

Secondary DNS Server: Enter the IP address of the alternate DNS server.

Domain Name: Enter the domain name.

WINS IP Address: Enter the WINS server's IP address (if present).

Lease Time: Select the length of time during which the DHCP assigned address will be in effect.

Note: The DHCP client will attempt to re-obtain its IP lease after half of the lease time has already expired. Using a low number will increase traffic on the network.

Using the Configuration Utility (continued)

Public LAN > VLAN > DHCP Configuration (continued)

Enable DHCP Server (continued):

Reserved IP Address List: If you want to use the Reserved IP Address List function, please click the hyperlink of the Reserved IP Address List on the management interface. Then, the setup of the Reserved IP Address List as shown in the following figure will appear. Please enter the related Reserved IP Address, MAC, and description (optional) on the management interface. After the information is entered, click **Apply** to complete the setup.

Reserved IP Address List -- Public LAN			
Item	Reserved IP Address	MAC	Description
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

(Total:40) First Previous Next Last

Enable DHCP Relay: In order to enable the DHCP Relay Mode, you must specify a DHCP server IP address.

Using the Configuration Utility (continued)

System Configuration > Private LAN Configuration

Private LAN Configuration		
Private LAN Port	Specific Route Profile	None
	Mode	NAT
	IP Address	192.168.0.40 *
	Subnet Mask	255.255.255.0 *
DHCP Server Configuration	○ Disable DHCP Server	
	⊙ Enable DHCP Server	
	DHCP Scope	
	Start IP Address	192.168.0.1 *
	End IP Address	192.168.0.100 *
	Primary DNS Server	*
	Secondary DNS Server	
	Domain Name	dlink.com *
	WINS IP Address	
	Lease Time	1 Day
	Reserved IP Address List	
	○ Enable DHCP Relay	

For an explanation of each field on this screen, please see the previous screen:
System Configuration > Public LAN Configuration.

Using the Configuration Utility (continued)

User Authentication

User Authentication allows the DSA-5100 owner/operator to control who has or does not have access to the Internet. The DSA-5100 can support five different authentication types simultaneously.

User Authentication > Authentication Policies

The DSA-5100 provides a simple interface to allow the administrator to easily complete the complicated management setup. The system provides a total of 5 authentication setups. The administrator can adopt different authentication methods corresponding to each management setup. Each management setup can use at most 20 management rules to go with the group configuration, so that the management of general users can be both diversified and flexible.

The administrator can select the desired management setup through the pull-down menu.

Authentication Policies Configuration					
Item	Policy Name	Status	Default	Group	
1	postfix1	Enabled	Yes	1	Edit
2	postfix2	Enabled	No	1	Edit
3	postfix3	Enabled	No	1	Edit
4	postfix4	Enabled	No	1	Edit
5	postfix5	Enabled	No	1	Edit

Item: Provides 5 sets of authentication policies.

Policy Name: The name of the policy can be modified here.

Status: **Enable** or **Disable** the policy.

Default: Select **Yes** for the default setup.

Group: Currently assigned group.

Edit: Click **Edit** to edit the policy.

Using the Configuration Utility (continued)

Edit Authentication Policies

Authentication Policies Configuration	
Policy ID	4:postfix4 ▾ Set as Default: ☐
Policy Name	postfix4 *(It's postfix name)
Policy Status	⊙ Enable ○ Disable
Black List Profile	None ▾
Authentication Server	⊙ Local ○ POP3 ○ RADIUS ○ LDAP ○ NT Domain Local Users List Assign to Group: 1:Group1 ▾ Exception Configuration ⊙Enable ○Disable Edit

Authentication Policy: Displays the system's preferred authentication method.

Policy ID: Select the policy you wish to edit here.

Set as Default: Make this selection to set the policy you have chosen to be the default Authentication policy.

Policy Name: Enter the postfix policy name.

Policy Status: Select **Enabled** or **Disabled** to activate or deactivate the selected policy.

Black List Profile: Enter the profile name to be blacklisted.

Authentication Server

The authentication server provides 6 authentication modes:
Local, POP3, RADIUS,LDAP,NT Domain, and External Web Server.

Assign to Group: Assign a group to the control group from the pulldown menu.

Exception Configuration: When you enable this feature you can exclude accounts from restrictions using the Edit feature. (This feature is displayed on the following page.)

Using the Configuration Utility (continued)

Authentication Server> Exception Configuration

Exception Configuration				
If	Attribute	Logic	Value	Group
1		equal to ∨		1: ∨
2		equal to ∨		1: ∨
3		equal to ∨		1: ∨
4		equal to ∨		1: ∨
5		equal to ∨		1: ∨

(Total:20) First Previous Next Last

Attribute: After the authentication, the DSA-5100 will obtain the user's attributes related to the authenticated server. The administrator can use certain attributes as the management rule for the setup.

Logic: Logic options include **equal to, not equal to, larger than, smaller than,** and **include**.

Value: Please fill in the desired value after the **attribute** and **logic** fields have been completed.

Group: Specifies the priority.

Default Group: When a user does not match the management rule logon, this priority rule will be applied.

⚠️ **Warning:** The policy name cannot include: GRIC, MAC, IP

Using the Configuration Utility (continued)

Authentication Methods>Local>Local Users List

The user's account information is stored in the DSA-5100. If you need to manage the user's account, please click the hyperlink **Local Users List** on the Authentication Server interface to enter into the Account Management Interface, shown below.

User List: It provides a complete list of existing user accounts, including information such as **Username, Password, MAC, Max Bandwidth, Request Bandwidth, Group,** and **Remark**. The administrator can delete or search for a single user from this management interface.

(Note: Max Bandwidth is the amount of maximum transmission capacity available on a network at any point in time. Request Bandwidth represents the amount of minimum transmission capacity that is available on a network at any point in time.)

Delete All: Click here to delete all user accounts**.**

Edit: To edit the content of an individual user account, click the hyperlink of the selected user account to enter the edit mode.

Refresh: Click here to show the most updated user account information

Authentication Methods > Local > Local Users List > Add User

Add User:

Create new accounts,including **Username** (mandatory), **Password** (mandatory) and **MAC** (optional), Max Bandwidth (optional), Request Bandwidth (optional) and assign to a user group.

Edit Account:

Make changes to the account by clicking on the **Username**. When the screen on the next page appears, edit the account information.

Using the Configuration Utility (continued)

Authentication Methods > Local > Local Users List > Add User> Edit Account

Edit Account:
Edit the account here.

Edit Account

Username	Amber *
Password	mypwd *
MAC	
Max Bandwidth	Unlimited
Request Bandwidth	None
Group	None
Remark	

Submit   Reset

Back to Users List

Local Users List > Add User> Upload User Account

Upload User Account:

Click the **Browse** button to select the text file for the user account. Click **Submit** to complete the

Note: The format of each line is "ID,Password,MAC,Max bandwidth,Request bandwidth,Group,Remark" without the quotes. There must be no space between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will be replaced by the new ones.

Upload User Account
File Name [   ] Browse...
Submit

upload. The format of the uploaded file should be a text file. Each line represents a User Account. The format is Username, Password, MAC, Remark. Each parameter is separated by a comma, and no space is allowed between MAC,Remark, but a comma is still needed.

Local Users List > Add User> Download User Account

Download User Account:

Click the **Download User Accounts** to view a list of all the user accounts. To save a new file, click **download.**
Click **download** to load accounts into your computer.

Users List						
Username	Password	MAC	MAX Bandwidth	Request Bandwidth	Group	Remark
Amber	pwd01		0	0	0	
Joy	pwd02		0	0	1	
Todd	pwd03		0	0	3	
Jennifer	pwd04		0	0	5	

download

30

Using the Configuration Utility (continued)

Authentication Methods > POP3

If a POP3 Server is used for user authentication, select POP3 in the interface shown here. The setup for the primary server or the secondary server (optional) is available. Enter the IP address or domain name of the Primary POP3 Server and its Primary POP3 Server port. Click **Apply** to enable the setting.

Enable SSL Connection: If you select this option, the authentication will be done by POP3 Protocol with SSL Username/Password encryption.

Authentication Methods > RADIUS

The DSA-5100 supports RADIUS Client to work with an existing RADIUS server.(Primary is required; Secondary is optional.)

802.1X Authentication: Select to enable 802.1X (in conjunction with a switch or AP that supports 802.1X). Click **Edit** to enter into the edit interface of 802.1X.

Trans Full Name:

Enable: ID and postfix will transfer to the RADIUS server for authentication, e.g., user@postfix1.

Disable: Only the ID will transfer to the RADIUS server for authentication. (e.g., user).

Class Configuration: Configuration reads parameters from a configuration file and returns their values on demand. Set the Max Bandwidth and Request Bandwidth, and assign group for every class.

Server IP: Provide the RADIUS server IP Address or Domain Name.

Authentication Port: The authentication port for the RADIUS server.

Accounting Port: The port reading the accounting information.

Secret Key: This is for encryption and decryption, must be configured on both RADIUS Server and DSA-5100.

Accounting Service: Select to enable the accounting service (optional).

Using the Configuration Utility (continued)

Authentication Methods > LDAP

You may configure a primary and a secondary server for LDAP authentication. If you select the LDAP authentication method, type in the IP Address (Domain

Name), Port number, the Base DN Data of LDAP Server, and select one of the Account Attribute Type. If you want to access the data from some LDAP servers which need to be authenticated, you have to enter the *username* and *password* in the **"Bind RDN"** and **"Bind Password"** fields, or check *"Anonymous Bind"* to just access the LDAP servers which don't need to be authenticated. Click **Apply** to save the changes.

Authentication Methods > NT Domain

Server IP Address: Enter the IP address of the Domain Controller Server.

Transparent Login: Select **Enable** or **Disable**.

Assign to Group: Select the group from the pulldown menu.

> ⚠ **Caution:** The NT Domain feature supports only a Windows 2000 controller. To use NT Domain Authentication please ensure the following conditions:
> 1. The WAN1 port preferred DNS server IP address must be the same as the Domain Controller Server IP address.
> 2. The Free Surfing List must also contain the Domain Controller Server IP address.
> 3. The Policy name must be your complete Domain name.

Using the Configuration Utility (continued)

External Web Server

External Authentication Configuration	
Protocol	⦿ HTTP ○ HTTPS
Server IP	
Server Port	80
Login Page	

The DSA-5100 supports an external web server function (including database) which enables a user to put the login page on an external web server, and change the login page anytime.

Protocol: Choose from http or https (http protocol is selected here).

Server IP: External Web server IP.

Server Port: External Web server Port number.

Login Page: Login page URL.

User Authentication>Group Configuration

Group Configuration						
Item	Group Name	Firewall Profile	Specific Route Profile	Schedule Profile	Bandwidth	
Guest	Guest	Global	Global	Schedule1	Unlimited	Edit
1	Group1	Global	Global	Schedule1	Unlimited	Edit
2	Group2	Global	Global	Schedule1	Unlimited	Edit
3	Group3	Global	Global	Schedule1	Unlimited	Edit
4	Group4	Global	Global	Schedule1	Unlimited	Edit
5	Group5	Global	Global	Schedule1	Unlimited	Edit

The administrator can configure 5 group profiles and a guest profile here. Click **Edit** next to the group that you want to configure and the screen on the next page will appear.

Using the Configuration Utility (continued)

User Authentication>Edit Group Configuration

Group Configuration	
Group Name Guest :	Guest
Firewall Profile	Global : Global
Specific Route Profile	Global : Global
Schedule Profile	1 : Schedule1
Total Bandwidth	Unlimited

Group Name Guest: Assign a group name; **Guest** is selected here.

Firewall Profile: Select the firewall profile for this group.

Specific Route Profile: Select the route profile for this group.

Schedule Profile: Select a schedule for this profile.

Total Bandwidth: Select the bandwidth limit that goes with this group.

User Authentication>Black List Configuration

Black List Configuration		
Select Black List :	1:Blacklist1	
Name	Blacklist1	
User	**Remark**	Delete
		(Total:0) First Prev Next Last
	Add User to List	

The administrator can manage a blacklist of up to 40 users. When a blacklisted user attempts to logon, he will be denied access.

Select Black List: Select the blacklist from the pulldown menu.

Add User to List: Click on this link and the interactive screen on the next page will appear.

Using the Configuration Utility (continued)

User Authentication>Black List Configuration

No	Username	Remark
	Add Users to Blacklist : Blacklist1	
1	b1	b1
2		
3		
4		
5		
6		
7		
8		
9		
10		

Username: Enter the username to be blacklisted here.

Remark: Add a comment (optional).

Apply: Click **Apply** to add the user to the blacklist.

Previous: Click **Previous** to return to the Black List Configuration.

Using the Configuration Utility (continued)

User Authentication>Black List Configuration>Delete a User

Black List Configuration		
Select Black List : 1:Blacklist1 ▾		
Name	Blacklist1	
User	**Remark**	Delete
b1	b1	☐
		(Total: 1) First Prev Next Last
	Add User to List	

Delete: To delete a user, check the box in the Delete column, and then click the

   Delete button.

No notification will appear to confirm the deletion.

User Authentication>Guest User Configuration

Guest User Configuration	
Guest User	⦿ Enable ○ Disable
	Guest User List
	Session Length 6 ▾ Hours
	Idle Timer : 600 Min(s) (1 - 1440)

Enable: Select **Enable** to activate the Guest Account feature for visitors.

Guest User List: Click to view the interactive screen (shown on the next page). Up to 10 guest accounts can be defined.

Session Length: You have the option to limit the guest's session time from 1-12 hours. By default, there is no limit to a guest's session.

Idle Timer: When enabled, on-line users who become inactive on the network after a specified period of time will be logged out automatically. The period can range from 1-1440 minutes. Ten minutes is the default value.

Using the Configuration Utility (continued)

User Authentication>Guest User List

Password:

Enter a password to
activate a guest
account. Up to ten
guest accounts can be
defined.

Guest User List		
Item	Username	Password
1	guest1	
2	guest2	
3	guest3	
4	guest4	
5	guest5	
6	guest6	
7	guest7	
8	guest8	
9	guest9	
10	guest10	

User Authentication>Roaming Configuration

The system provides Airpath and Pronto Service for roaming. Set up the parameters
in this page to let the user of the Airpath and Pronto Service use the DSA-5100.
Click Apply.

Roaming Configuration		
Airpath	☑ Enable Airpath	
	Airpath Server	Free Surfing Area
	Device name	*
	Server IP	*
	Authentication Port	*
	Accounting Port	*
	Secret Key	*
	Accounting Service	Enabled
	Authentication Method	PAP
	Default Group	1:Group1
	Upload Certificate	
Pronto	☐ Enable Pronto	

⚠ **Caution:** The login location is the same as the location of the account's
origin. For example if the account was opened in Los Angeles, then the
login location is Los Angeles.

37

1. Airpath:

User who registered Airpath Wireless's service can login local public network via roaming in. Within system default login page, DSA-5100 provide roaming user with a link redirected to Airpath's login page. Some free surfing website can also be specified in the Free Surfing Area. DSA5100's administrator should contact with your Airpath's agent about the server's configuration before switched on the feature.
To configure Airpath's, system also allow administrator upload customer preferred private key and certification.

Roaming Configuration		
	☑ Enable Airpath	
	Airpath Server	Free Surfing Area
	Device name	[ ] *
	Server IP	[ ] *
	Authentication Port	[ ] *
Airpath	Accounting Port	[ ] *
	Secret Key	[ ] *
	Accounting Service	Enabled ▼
	Authentication Method	PAP ▼
	Default Group	1:Group1 ▼
	Upload Certificate	

Airpath Server: Users can access these websites prior to authentication. This function is used for advertising or other purposes.
Device Name: FQDN (Fully-Qualified Domain Name). This is the domain name of the DSA-5100 as seen on client machines connected on LAN ports. A user on client machine can use this name to access DSA-5100 instead of its IP address.
Server IP: IP address of Airpath RADIUS server.
Authentication Port: Airpath RADIUS server authentication port.
Secret Key: Airpath RADIUS server secret key.
Accounting Service: Enable or disable RADIUS accounting service.
Authentication Method: Select Challenge Handshake Authentication Protocol (CHAP) or Plain Authentication Protocol (PAP).
Default Group: Set a group as the default group.
Upload Certificate: The DSA-5100 allows the user to upload customer certification. (The key must be in key format and the certificate must be in certificate format.)

2. Pronto:

DSA-5100 can also be configured for Pronto Networks and accept roaming users from Pronto Networks To facilitate DSA-5100 for Pronto registered users, administrator simply enables Pronto Service and enters basic Pronto Network Server information. DSA-5100 will automatically configure itself and register with Pronto Networks using these information. DSA-5100 is fully operational with Pronto Networks upon successful device registration and restart.

Roaming Configuration		
Airpath	☑ Enable Airpath	
	Airpath Server	Free Surfing Area
	Device name	[_____] *
	Server IP	[_____] *
	Authentication Port	[_____] *
	Accounting Port	[_____] *
	Secret Key	[_____] *
	Accounting Service	Enabled ▼
	Authentication Method	PAP ▼
	Default Group	1:Group1 ▼
	Upload Certificate	

HNS Server: This is the fully specified URL to be used as the end-point for web service communication.

NAT Server IP: IP address of Network Address Translation Server

NAT Server Port: Communication port of Network Address Translation Server

Heartbeat Interval: This is an integer value specifying the interval in seconds at which the Agent process will send a Heartbeat message to HNS. This will also be the interval at which HNS is polled for commands to be executed on the AP. Setting this value to 0 will stop Heartbeat. Setting this value > 0 will force the Heartbeat to occur once every heartbeat interval seconds, overriding the default value and the recommended value received from HNS.

Default Group: Set a group as the default group.

Pronto Server (Free Surfing Area): users can access these websites prior to authentication. This function is used for advertising or other purposes.

Login page URL: Pronto login page URL

Login fail page URL: Pronto login fail page URL

Login successful page URL: Pronto login successful page URL for feature release

Using the Configuration Utility (continued)

Primary / Backup Server (setting from Pronto):

> Authentication Server IP: IP address of Pronto RADIUS server

> Authentication Port: Pronto RADIUS server authentication port

> Authentication Secret Key: Pronto RADIUS server authentication secret key

> Accounting Server IP: IP address of Pronto RADIUS accounting server

> Accounting Port: Pronto RADIUS server accounting port

> Accounting Secret Key: Pronto RADIUS server accounting secret key

> Accounting Service: Enable or disable RADIUS accounting service

> Authentication Method: Challenge Handshake Authentication Protocol (CHAP) or Plain Authentication Protocol (PAP).

User Authentication>User Control

Logout Timer: If a user is idle and has not used the network for the configured time, the system will automatically log out the user. The logout time can be set from 1-1440 minutes. The default logout time is 10 minutes.

User Control	
Idle Timer	10 Min(s) (1 - 1440)
Multiple Login	○ Enable ⊙ Disable
Friendly Login	⊙ Enable ○ Disable 12 Hours ▾
Friendly Logout	○ Enable ⊙ Disable
WAN Fail Testing URL	http://
WAN Fail	⊙ Pass ○ Block
POP3 Message	Edit Mail Message
MAC Address Control	⊙ Enable ○ Disable MAC Address List

Multiple Login:
After you have selected this function, the user with the same ID can logon from several computers.

Friendly Login:
After you select this function, the logon page will automatically obtain the username and password from the previous authentication logon. The user no longer needs to click the button to login. If this option is not selected, the user has to click **Login** and enter the username and password (which will be saved for 12 hours).

Using the Configuration Utility (continued)

User Authentication>User Control (continued)

Friendly Logout:

When a user logs on, a small window will appear, showing the user information and providing him or her with a button for logout. If this option is enabled, it will close the window and logout the user. If you do not select this option, closing the window will not log out the user. To logout, browse to https://1.1.1.1/logout.shtml

WAN Fail Testing URL:

When the WAN connection fails, the user login screen will be redirected to the URL. The DSA-5100 can detect if the WAN connection fails by using an ICMP echo mechanism to ping the default gateway and the DNS server periodically.

Pass: Allows free access without control.
Block: Displays the error message and blocks all access. (More secure.)

POP3 Message:

Before a user logs on to the system with the username and password, the user may receive a welcome e-mail. If you want to set the content of the e-mail, please fill in the text in the table shown here.

MAC Address Control:

When MAC Address Control is enabled, only 40 users can connect to the Authentication Port and login to the DSA-5100 if they have previously registered their MAC Address in MAC Address Control. Please refer to the configuration screen shown here.
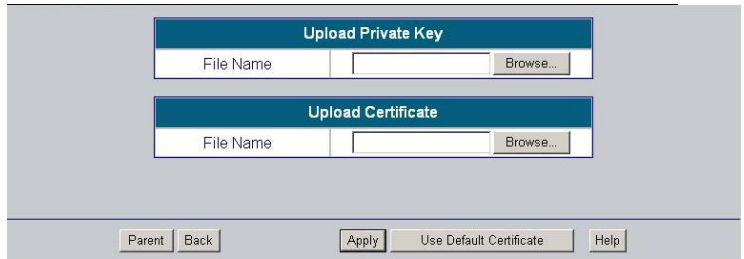
> ⚠ The format of the MAC address can be XX:XX:XX:XX:XX:XX or XX-XX-XX-XX-XX-XX.

Using the Configuration Utility (continued)

User Authentication>Upload File

Private Key/ Certification:
The DSA-5100 allows the user to upload certification. (The key must be in key format and the certificate must be in certificate format.)

Upload Private Key

| File Name | | Browse... |

Upload Certificate

| File Name | | Browse... |

Parent Back   Apply   Use Default Certificate   Help

File Name:
Enter the filename of the logon Web page or click **Browse** to browse for the file on your local PC.

Upload Login Page

| File Name | | Browse... |

Submit   Use Default Page

Use default page:
Click to recover the factory default setting of the logon interface.

Submit:
Click to begin uploading the page.

Preview:
After the upload is completed, click Preview (at the bottom of the page) to preview the user-defined logon interface.

HTML codes:
The user-defined login interface must include the following HTML code to provide a channel for the user to key in the username and password:

```
<form action="userlogin.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Enter">
<input type="reset" name="clear" value="Clear">
</form>
```

Using the Configuration Utility (continued)

User Authentication>Upload Logout Page>HTML codes

Use the following HTML codes for the User Logout Interface:

```
<form action="userlogout.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Logout">
<input type="reset" name="clear" value="Clear">
</form>
```

Upload Error Page

To provide a custom user login error page, please specify the file name to upload to the DSA-5100. If you want to get back to the **Error** page, click **Use Default Page**. If you want to display the Login Error Page, click **Preview**.

Upload Login Successful Page

To provide a custom user login succeed page, please specify the file name to upload to the DSA-5100. If you want to get back to the **Succeed** page, click **Use Default Page**. If you want to display the Login Succeed Page, click **Preview**.

Upload Logout Successful Page

To provide a custom user **Success** page, please specify the file name to upload to the DSA-5100. If you want to get back to the default user **Success** page, click **Use Default Page**. If you want to display the Logout Succeed Page, click **Preview**.

43

Using the Configuration Utility (continued)

The DSA-5100 provides three kinds of Profile configurations, including Firewall Profile, Specific Route Profile, and Login Schedule Profile.

Group Profile > Firewall Profile

Global is the default setting. Use the Global setting to apply parameters to all users. There are 5 individual profiles available also.

Profile Name:
To give a name to the Firewall Profile.

Filter Rule Item:
Click the number to edit the filter rule.
The window below will appear.

Firewall Profile							
Filter Rule Item	Name	Active	Action	Source	Destination	Protocol	MAC
1		☐	Pass	ANY	ANY	ALL	
2		☐	Block	ANY	ANY	ALL	
3		☐	Block	ANY	ANY	ALL	
4		☐	Block	ANY	ANY	ALL	
5		☐	Block	ANY	ANY	ALL	
6		☐	Block	ANY	ANY	ALL	
7		☐	Block	ANY	ANY	ALL	
8		☐	Block	ANY	ANY	ALL	
9		☐	Block	ANY	ANY	ALL	
10		☐	Block	ANY	ANY	ALL	

Profile ID: Default:Global
Profile Name: Global

Group Profile > Firewall Profile>Edit Filter Rule

Rule Name:
The name of the IP filter rule.

Enable this Rule:
Check to enable this rule.

Action:
Specifies the action to be taken when packets match the rule.

Edit Filter Rule
Profile Name: IP Filter 1
Rule Item: 1
Rule Name: ☐ Enable this Rule
Action : Block ▾   Protocol ALL ▾
Source MAC Address: (For Specific MAC Address Filter, ex:00:00:00:00:00:00)

	Interface	IP	Subnet Mask	Start Port End Port
Source	ALL ▾	1.2.3.4	255.255.255.255 (/32) ▾	
Destination	ALL ▾		255.255.255.255 (/32) ▾	

Pass: Packets matching the rule will be passed.

Block: Packets matching the rule will be dropped.

Protocol:
Provides three kinds of protocols: **TCP**, **UDP**, and **ICMP**. Select **All** to apply all three protocols.

Using the Configuration Utility (continued)

Group Profile > Firewall Profile>Edit Filter Rule (continued)

Source MAC:
MAC address of the Network component sending the request.

Source (Destination) Interface:
Source (Destination) Interface includes 4 interfaces: WAN1, WAN2, Public LAN, and Private LAN. Select ALL to apply to all four interfaces.

Source (Destination) IP Address:
IP address of the Network component sending (receiving) the request.

Source (Destination) Subnet Mask:
Subnet Mask of the Network component sending (receiving) the request.

Source (Destination) Operator:
Provides the comparison rules: =(Equal), != (Not Equal), >(Larger Than), and <(Less Than).

Source (Destination) Start Port:
Start Port of the Network component sending (receiving) the request.

Source (Destination) End Port:
End Port of the Network component sending (receiving) the request.

Using the Configuration Utility (continued)

Group Profile > Specific Route Profiles

If you want networks to have
access to each other, you
should add a specific route in
the DSA-5100.

Profile Name:
Name the specific route profile.

Destination IP Address:
Specifies the target network or
host IP

Subnet Netmask:
Specifies the target subnet
mask.

Gateway IP Address:

Specifies the IP address of the next hop router.

Specific Route Profile				
Global:Global ∨				
Profile Name: Global				
Route Item	Destination		Gateway	Default
	IP Address	Subnet Netmask	IP Address	
1		255.255.255.255 (/32) ∨		☐
2		255.255.255.255 (/32) ∨		☐
3		255.255.255.255 (/32) ∨		☐
4		255.255.255.255 (/32) ∨		☐
5		255.255.255.255 (/32) ∨		☐
6		255.255.255.255 (/32) ∨		☐
7		255.255.255.255 (/32) ∨		☐
8		255.255.255.255 (/32) ∨		☐
9		255.255.255.255 (/32) ∨		☐
10		255.255.255.255 (/32) ∨		☐

> ⚠️ *Caution: To allow two machines to access data from each other, add a static route to the next connected router in order to send all packets back to the DSA-5100.*
>
> *After the static route is changed, it is necessary to restart the DSA-5100 to enable the static route.*

Using the Configuration Utility (continued)

Group Profile > Login Schedule Profiles

The user's login schedule can be set. After durations are defined, please click **Apply** to save the settings in the DSA-5100.

Login Schedule Profile							

Schedule ID: 1:Schedule1
Profile Name: Schedule1   ⦿ Enable ○ Disable

HOUR	SUN	MON	TUE	WED	THU	FRI	SAT
0	☑	☑	☑	☑	☑	☑	☑
1	☑	☑	☑	☑	☑	☑	☑
2	☑	☑	☑	☑	☑	☑	☑
3	☑	☑	☑	☑	☑	☑	☑
4	☑	☑	☑	☑	☑	☑	☑
5	☑	☑	☑	☑	☑	☑	☑
6	☑	☑	☑	☑	☑	☑	☑
7	☑	☑	☑	☑	☑	☑	☑
8	☑	☑	☑	☑	☑	☑	☑

Network Configuration > Network Address Translate

DMZ

If you have several IP addresses, you can assign them to the WAN port of the system. You can define at most 40 Public IPs for the corresponding combination at the Ethernet end (Virtual IP Address) and WAN end (Public IP Address). The WAN port of the system will automatically set the public address defined here. These settings will be effective immediately after you click the **Apply** button.

	DMZ	
Item	Internal IP Address	External IP Address
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

(Total:40) First Prev Next Last

Virtual Server

The function of this item permits you to define at most 40 virtual servers, so that computers may access LAN resources from the WAN interface. The Virtual Server function also allows one to specify the type of traffic allowed, TCP, UDP or both. These settings will be effective immediately after you click **Apply**.

		Virtual Server			
Item	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1				○ TCP ○ UDP	☐
2				○ TCP ○ UDP	☐
3				○ TCP ○ UDP	☐
4				○ TCP ○ UDP	☐
5				○ TCP ○ UDP	☐
6				○ TCP ○ UDP	☐
7				○ TCP ○ UDP	☐
8				○ TCP ○ UDP	☐
9				○ TCP ○ UDP	☐
10				○ TCP ○ UDP	☐

(Total:40) First Prev Next Last

Using the Configuration Utility (continued)

Network Configuration > Network Address Translate (continued)

Port and IP Redirect

When any user attempts to connect to a destination defined in this interface, the connection packet will be converted to the corresponding destination. You can define up to 40 groups for redirection on this interface. These settings will be effective immediately after you click **Apply**.

		Port and IP Redirect			
Item	**Destination**		**Translated to Destination**		**Type**
	IP Address	Port	IP Address	Port	
1					○TCP ○UDP
2					○TCP ○UDP
3					○TCP ○UDP
4					○TCP ○UDP
5					○TCP ○UDP
6					○TCP ○UDP
7					○TCP ○UDP
8					○TCP ○UDP
9					○TCP ○UDP
10					○TCP ○UDP

(Total:40) First Prev Next Last

Network Configuration > Privilege List

IP Pass Through Configuration

To permit a specific device at the user end to have network access without going through authentication, you only need to key in the IP address of the user on this interface. This system permits at most 100 IP addresses to have network access without going through authentication. These settings will be effective immediately after you click **Apply**.

	IP Pass Through Configuration	
Item	**Privilege IP Address**	**Remark**
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

(Total:100) First Prev Next Last

> **Warning:** Permitting specific IP addresses to have network access rights without going through authentication may cause security problems.

Using the Configuration Utility (continued)

Network Configuration > MAC Pass Through Configuration

You can also bypass authentication based on the MAC address at the user end. Please enter the MAC address of the user on this interface. This system permits at most 100 MAC addresses to have network access rights without going through authentication. The format of the MAC address is XX:XX:XX:XX:XX:XX.

These settings will be effective immediately after you click **Apply**.

> ⚠️ **Warning:** *Permitting specific MAC addresses to have access rights without going through authentication may cause security problems.*

Network Configuration > Monitor IP List

The system will send out the packet regularly to monitor the connection status of the IP addresses on the list. If the monitored IP address does not respond, the system will send an e-mail to the administrator. After enter the related information and click Apply, these settings will be effective immediately. You can click Monitor to check the current status of all the monitored IP. The system provides 40 IP addresses a most on the "Monitor IP List" to set.

49

Using the Configuration Utility (continued)

Network Configuration > Monitor IP List (continued)

Notify Configuration

From: The e-mail address of the administrator server in charge of the monitoring.

To: The e-mail address of the user of the IP address under the monitoring.

Interval: The time interval to send the e-mail report.

SMTP Server: The IP address of the SMTP server.

Auth Method: Providing 5 authentication methods: None, PLAIN, LOGIN, CRAM-MD5, and NTLMv1.

> NTLMv1 is not currently available for general use.

> PLAIN and CRAM-MD5 are standardized authentication mechanisms, while Login and NTLM are Microsoft proprietary mechanisms. Only PLAIN and LOGIN can use the UNIX login password. Netscape uses PLAIN. Outlook and Outlook express default to using LOGIN, although they can be set to use NTLMv1.

> Pegasus uses CRAM-MD5 or LOGIN but you are not able to configure which to use.

> Eudora possibly uses NTLMv1, perhaps LOGIN that have not been verified.

Network Configuration > Free Surfing Area

The Free Surfing Area permits users to logon to certain websites or Domains before passing through authentication. You can enter up to 20 IP addresses (or Domain Names) into the Free Surfing Area. This function allows you to provide potential users a free network experience, while introducing them to your site. All unauthenticated requests to servers not on the list will be dropped.

Free Surfing Area			
Item	Address	Item	Address
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

Using the Configuration Utility (continued)

Network Configuration > Proxy Server Properties

Internal Proxy Server:
Enable this function to configure the DSA-5100 as a proxy server.

External Proxy Server:

By default, only port 80 is allowed. It will appear on the login Web page. If you have built a Proxy Server in your network environment, and the user's browser is set to Proxy, you must set your External Proxy Server IP address and Proxy Port in this section fo the configuration in order to operate in the Proxy network environment.

Internal Proxy Server	
Built-in Proxy Server	○ Enable ⊙ Disable

External Proxy Server		
Item	Server IP	Port
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Using the Configuration Utility (continued)

Utilities > Change Password

DSA-5100 provides 2 built-in user accounts: **admin** and **manager**.

admin: This user is the administrator in the DSA-5100.
manager: This user has the right to manage a user account, the admin functions are denied.

The **admin** and **manager** can change their passwords; specify the current password first. The new password must be entered twice.

Change Admin Password	
Old Password	
New Password	
Verify Password	

Change Manager Password	
Old Password	
New Password	
Verify Password	

> *Note: If you lost or forgot the Administrator's Password, you can reset it through the text mode management interface of the serial port.*

Using the Configuration Utility (continued)

Utilities > Backup/Restore Strategy

This utility provides the backup function, and the ability to restore backup settings. This function can also restore the factory default settings to the system.

Backup / Restore Strategy
Create Backup Image
Create
Restore System Settings From File
[   ] Browse...
Restore
Reset to the Factory-Default Settings
Reset

Create Backup Image: **Create:** Generate the backup (image) file.

Restore Settings From File: **Browse:** Browse for the backup file.
Restore: Click to load the selected backup file
for the setup status.
(**Caution:** The image file must be generated by the
the system).

Reset to the Factory-Default   Restore to the factory default setting of the system.
Setting:

53

Using the Configuration Utility (continued)

Utilities > Firmware Upgrade

You may obtain firmware upgrades from D-Link's support website:
http://support.dlink.com

Firmware Upgrade	
Current Version	1.0.0
File Name	[ ] [Browse...]

> ⚠ **Warning:** *A Firmware upgrade may cause data loss on setup. Please refer to the version description to see if there is any limitation before upgrading your firmware.*

Click **Browse** to browse the files. After you have found the firmware, click **Submit** and the browser will upload the file to the system. The system will start upgrading the firmware.

You must restart the system before the firmware upgrade is effective. If you have modified any setting, remember to save the setting before restarting the system.

> ⚠ **Warning:** *Please restart the system through the management interface. Do not turn off the system directly and then turn on the power again. (Doing so may damage the unit.)*

Utilities > Restart

This function allows you to safely restart the system. It takes about one minute.

OFF: If you need to turn OFF the power, we recommend that you first RESTART the system, and then turn OFF the power, AFTER you hear a beep.

Do you want to restart DSA-5100?

[YES] [NO]

> ⚠ **Warning:** *All online users connected to the system will be disconnected when the system is restarted.*

Using the Configuration Utility (continued)

Status> System Status

You can use this function to get the overview of the system status. Please refer to the following example.

System Status		
	Current Firmware Version	1.10.A5
	System Name	DSA-5100
	Admin info	N/A
	Succeed Page	http://www.dlink.com
	External Syslog Server	N/A:N/A
	Proxy Server	Disabled
	WAN Fail	Block
Manage	Remote Management IP	0.0.0.0/0.0.0.0
	SNMP	Disabled
History	Retained Days	3 Days
	Email To	N/A
Time	External Time Server	tock.usno.navy.mil
	Date Time(GMT+0:00)	Fri, 13 Jan 2006 16:59:42 +0800
User	Idle Timer	10 Min(s)
	Multiple Login	Disabled
	Guest Account	Disabled
DNS	Primary DNS Server	168.95.1.1
	Secondary DNS Server	N/A
Friendly	Login	Disabled
	Logout	Disabled

Using the Configuration Utility (continued)
Status> System Status (continued)

Item		Description
Current Firmware Version		The firmware version currently used by the DSA-5100.
System Name		System name - the default is DSA-5100.
Admin Info		Administrator's information will be shown on the logon screen when a user has a connection problem.
Succeed Page		The starting URL after a user logs on successfully.
Syslog to		The IP address and port number of the external Syslog server.
Proxy Server		Proxy Server is not set.
WAN Fail		When the connection at WAN is abnormal (WAN Fail), all online users can log on to the network.
Manage	Remote Management IP	It permits a specific IP address to set up the DSA-5100 from the WAN1 port.
	SNMP	Do not enable SNMP management function.
History	Retained Days	The system will retain the user information up to a maxi mum of 3 days.
	E-mail To	Send the history to this email address.
Time	Time Server Name	The DSA-5100 uses an external Time Server to check time.
	Date Time(GMT+0:00)	The system time is Greenwich time.
User	Idle Timer	It is the logout time for idling. The online user will be forced to logout after being idled for 10 minutes.
	Multiple Login	It does not allow multiple logins for a user.
	Guest Account	Enable the Guest Account.
DNS	Primary DNS server	Primary DNS Server IP Address.
	Secondary DNS server	Secondary DNS Server IP Address.
Friendly	Login	User must click "Login" to execute the login procedure. The system will not automatically get the username and password from the previous login for the direct authentication login.
	Logout	If a user logs in, a small window will show the user's information and provide a logout button for the logout. Selecting **Disable** ensures that closing the small window will not cause a logout to the user.

Using the Configuration Utility (continued)
Status> Interface Status

Interface Status		
WAN1	MAC Address	00:90:0B:02:43:45
	IP Address	10.2.3.233
	Subnet Mask	255.255.255.0
Public LAN	Mode	NAT
	MAC Address	00:90:0B:02:43:47
	IP Address	192.168.1.40
	Subnet Mask	255.255.255.0
	IP_PNP	Disabled
	Mobile IP	Disabled
Public LAN DHCP Server	Status	Enabled
	WINS Server	N/A
	Start IP Address	192.168.1.100
	End IP Address	192.168.1.200
	Lease Time	60 Min(s)
Private LAN	Mode	NAT
	MAC Address	00:90:0B:02:43:46
	IP Address	192.168.0.40
	Subnet Mask	255.255.255.0
Private LAN DHCP Server	Status	Enabled
	WINS Server	N/A
	Start IP Address	192.168.0.1
	End IP Address	192.168.0.100
	Lease Time	1440 Min(s)

Using the Configuration Utility (continued)

Status> Interface Status (continued)

Item		Description
	MAC Address	The MAC address of the WAN1 port
WAN1	IP Address	The IP address of the WAN1 port
	Subnet Mask	The Subnet Mask of the WAN1 port
	Mode	Public LAN port mode: NAT mode
	MAC Address	The MAC address of the Public LAN port
	IP Address	The IP address of the Public LAN port
Public LAN	Subnet Mask	The Subnet Mask of the Public LAN port
	IP PNP	Enable IP PNP on the Public LAN port
	Mobile IP	Enable Mobile IP on the Public LAN port
	Status	Enable the DHCP server on the Public LAN port
	WINS IP Address	Set the WINS server IP on the DHCP server
Public LAN DHCP Server	Start IP Address	The starting IP Address of the DHCP pool
	End IP address	The ending IP Address of the DHCP pool
	Lease Time	The lease time of the IP Address
	Mode	Private LAN port mode: NAT mode
	MAC Address	The MAC address of the Private LAN port
Private LAN	IP Address	The IP address of the Private LAN port
	Subnet Mask	The Subnet Mask of the Private LAN port
	Status	Enable the DHCP function on the Private LAN port
	WINS IP Address	Set the WINS server IP address on the DHCP server
Private LAN DHCP Server	Start IP Address	The DHCP pool starting IP address
	End IP address	The DHCP pool ending IP address
	Lease Time	The lease time of the IP address

Using the Configuration Utility (continued)

Status > Current Users

With this feature, you can obtain the information of each online user including Username, IP, MAC, Packets In, Bytes In, Packets Out, Bytes Out, and Idle Time. The administrator can use this function to force a specific online user to logout. If you want to force a user to logout, you only need to click the hyperlink **Logout** next to the online user's name.

			Current Users List						
Item	Username	IP Address	MAC Address	Pkts In	Bytes In	Pkts Out	Bytes Out	Idle	Logout

Refresh

Status > Traffic History

Notify Configuration:

History Email: The DSA-5100 will save the history into the internal DRAM. If you want to automatically send the history to your E-mail address, please enter your E-mail address in the History E-mail column.

Interval: The Interval column shows the interval for sending the history E-mail. If you choose one day, then the history mail will be sent to you once a day.

Syslog To: Specify the IP and Port of the Syslog server.

Notify Configuration		
	From:	
	To:	
History E-mail	Interval:	1 Hour
	SMTP Server:	
	Auth Method:	NONE
Syslog To	IP:	Port:

Traffic Histroy: Check the history of the system. The history of each day will be saved independently. This system will save the history in the DRAM for more than 3 days.

Date	Size (Byte)
2006-01-10	130
2006-01-11	65
2006-01-12	65
API History	
Date	Size (Byte)
2006-01-10	23
2006-01-11	23
2006-01-12	23

⚠️ *Caution: Since the history is saved in DRAM, if you need to restart the system and want to keep the history, please manually duplicate the history.*

Using the Configuration Utility (continued)

Status > Traffic History (continued)

If you have entered the Administrator's E-mail address in the system configuration interface, then the system will automatically send out the history of the previous day to that E-mail address.

The first line of the history is the title, and the actual history starts from the second line. Each line includes a record, and each record consists of 9 fields Date, Type, Name, IP, MAC, Packets In, Bytes In, Packets Out, and Bytes Out to show the history of each user.

Traffic History (2004-03-15)								
Date	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out

Console Interface

The DSA-5100 provides a serial interface for the manager to handle different problems and situations for the operation. To link to the Console interface of the DSA-5100, you need a null modem cable (provided). The terminal simulation program that you use, such as the Hyperterminal, should be set to the parameter value of 115200,8,n,1.

The main console is a basic interface using interactive dialog boxes. Please use the arrow keys on the keyboard to browse the menu and press the **Enter** key to select specific menus and confirm entered data.

Console Interface > Main Menu

Once you properly connect to the serial port of the DSA-5100, the console welcome screen will appear automatically. If the welcome screen does not appear in the terminal simulation program automatically, please press the **Down** arrow key, so that the terminal simulation program will send some commands to the serial port of the DSA-5100, and the welcome screen or the main menu will appear again. If you are still unable to see the welcome screen or the main menu of the console, please check if the connection of your cables and the setup of the terminal simulation program are correct.

```
            D-Link DSA - 5100 Basic Configuration
                 Please select functions:

        Utility   Utilities for network debugging
        Password  Change admin password
        Reset     Reload factory default
        Restart   Restart D-Link DSA - 5100



              <  OK  >        <Cancel>
```
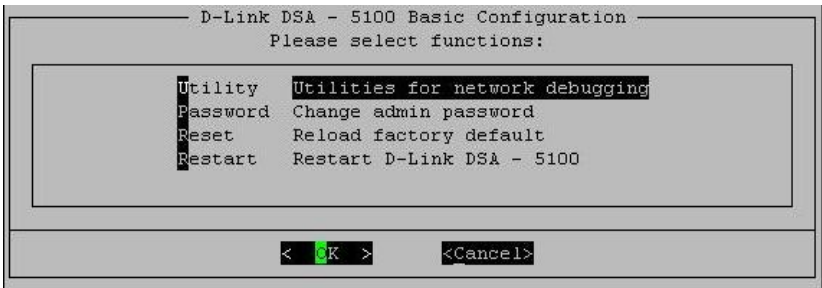
Using the Configuration Utility (continued)

Console Interface > Utilities for Network debugging

The DSA-5100 console interface provides several utilities to assist the Administrator. The utilities provided are described as follows:

```
┌───────── D-Link DSA - 5100 Configuration Utility ─────────┐
│                    Please select utility:                 │
│  ┌──────────────────────────────────────────────────────┐ │
│  │PING      Ping host(IP)                                │ │
│  │Trace     Trace routing path                           │ │
│  │ShowIF    Display interface settings                   │ │
│  │ShowRT    Display routing table                        │ │
│  │ShowARP   Display ARP table                            │ │
│  │UpTime    Display system up time                       │ │
│  │Status    Check service status                         │ │
│  │Safe      Set device into 'safe mode'                  │ │
│  │NTP       Synchronize clock with NTP server            │ │
│  │Main      Main menu                                    │ │
│  └──────────────────────────────────────────────────────┘ │
│                                                           │
│              <  OK  >          <Cancel>                    │
└───────────────────────────────────────────────────────────┘
```

Ping host (IP)
By sending an ICMP echo request, a specific target can be tested.
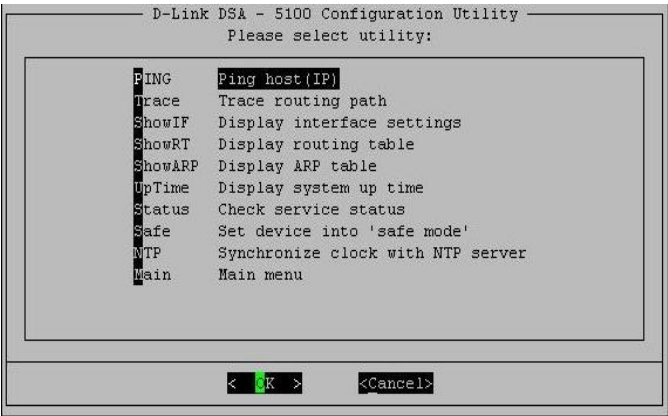
Trace routing path
Trace the routing path to a specific target.

Display interface settings
Displays each network interface setting including the MAC address, IP address, and netmask.

Display the routing table
The internal routing table of the DSA-5100 is displayed to assist the confirmation of the successful setup of another static route on the DSA-5100.

Display ARP table
The internal ARP table of the DSA-5100 is displayed.

Display system up time
The system up time of the DSA-5100 is displayed.

Check service status
The current status of each service on the DSA-5100.

Set device into 'safe mode'
If the administrator is unable to use the Web Management Interface, through a Web browser, then he/she can choose this utility and set the DSA-5100 into safe mode. The administrator can then manage this device with a Web browser again.

Synchronize clock with NTP server
Specify and immediately check and correct the clock through the NTP protocol and network time server. Since the DSA-5100 does not support manual setup for its internal clock, you need to configure the internal clock through NTP.

Using the Configuration Utility (continued)

Console Interface > Change Admin password

Besides supporting the use of a console management interface through the connection of the null modem, the DSA-5100 also supports the SSH online connection for the DSA-5100's setup. When using a null modem to connect to the DSA-5100 console, you do not need to enter the administrator's password.

When SSH is used to connect the DSA-5100, the username is **admin** and the default password is also **admin**. The set values are the same as those for the Web management interface. You can use this option to change the DSA-5100 administrator's password. If you forget the password and are unable to login to the console management interface of the DSA-5100, you can still use the null modem cable to connect directly to the console management interface of the DSA-5100. You will need to set the administrator's password again.

> ⚠️ **Caution:** When using SSH for connection, we recommend that you immediately change the DSA-5100 Admin username and password after you logon to the system for the first time, for security purposes.

Console Interface > Reload Factory Default

Resets the system to factory default settings.

Console Interface > Restart the DSA-5100

Restarts the DSA-5100.

Networking Basics

Using the Network Setup Wizard in Windows XP

In this section you will learn how to establish a network at home or work, using **Microsoft Windows XP.**

Note: Please refer to websites such as http://www.homenethelp.com and http://www.microsoft.com/windows2000 for information about networking computers using Windows 2000, ME or 98SE.

Go to **Start>Control Panel>Network Connections**
Select **Set up a home or small office network**

When this screen appears, click **Next.**

Networking Basics (continued)

Please follow all the instructions in this window:

Network Setup Wizard

Before you continue...

Before you continue, review the checklist for creating a network.

Then, complete the following steps:

- Install the network cards, modems, and cables.
- Turn on all computers, printers, and external modems.
- Connect to the Internet.

When you click Next, the wizard will search for a shared Internet connection on your network.

[< Back] [**Next >**] [Cancel]
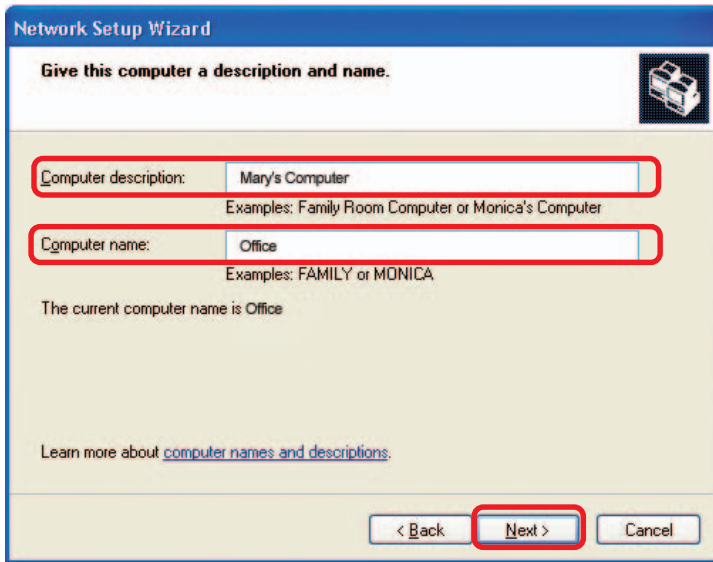
Click **Next.**

In the following window, select the best description of your computer. If your computer connects to the internet through a gateway/router, select the second option as shown.

Network Setup Wizard

Select a connection method.

Select the statement that best describes this computer:

○ This computer connects directly to the Internet. The other computers on my network connect to the Internet through this computer.
  View an example.

⦿ This computer connects to the Internet through another computer on my network or through a residential gateway.
  View an example.

○ Other

Learn more about home or small office network configurations.

[< Back] [**Next >**] [Cancel]

Click **Next.**

Networking Basics (continued)

Enter a **Computer description** and a **Computer name** (optional.)

Click **Next.**

Enter a **Workgroup** name. All computers on your network should have the same **Workgroup name.**

Click **Next.**

Networking Basics (continued)

Please wait while the **Network Setup Wizard** applies the changes.
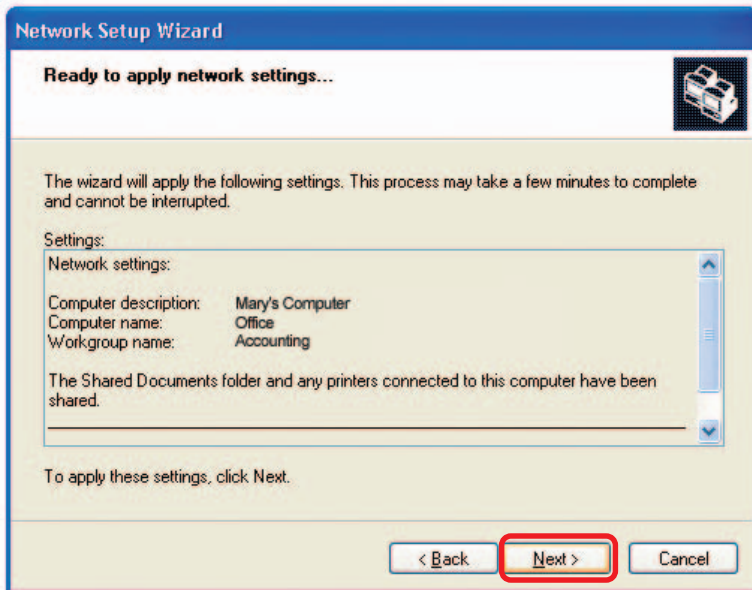
When the changes are complete, click **Next**.

Please wait while the **Network Setup Wizard** configures the computer.
This may take a few minutes.
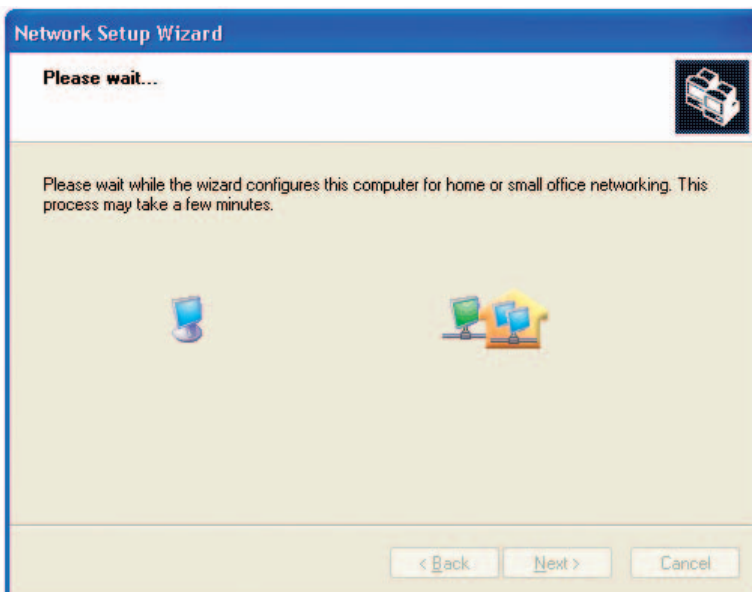
Networking Basics (continued)

In the window below, select the option that fits your needs. In this example, **Create a Network Setup Disk** has been selected. You will run this disk on each of the computers on your network. Click **Next**.

Network Setup Wizard

You're almost done...

You need to run the Network Setup Wizard once on each of the computers on your network. To run the wizard on computers that are not running Windows XP, you can use the Windows XP CD or a Network Setup Disk.

What do you want to do?

- ⦿ Create a Network Setup Disk
- ○ Use the Network Setup Disk I already have
- ○ Use my Windows XP CD
- ○ Just finish the wizard; I don't need to run the wizard on other computers

< Back   Next >   Cancel

Insert a disk into the Floppy Disk Drive, in this case drive **A.**

Network Setup Wizard

Insert the disk you want to use.

Insert a disk the into the following disk drive, and then click Next.

3½ Floppy (A:)

If you want to format the disk, click Format Disk.

Format Disk

< Back   Next >   Cancel

Click **Next.**

67
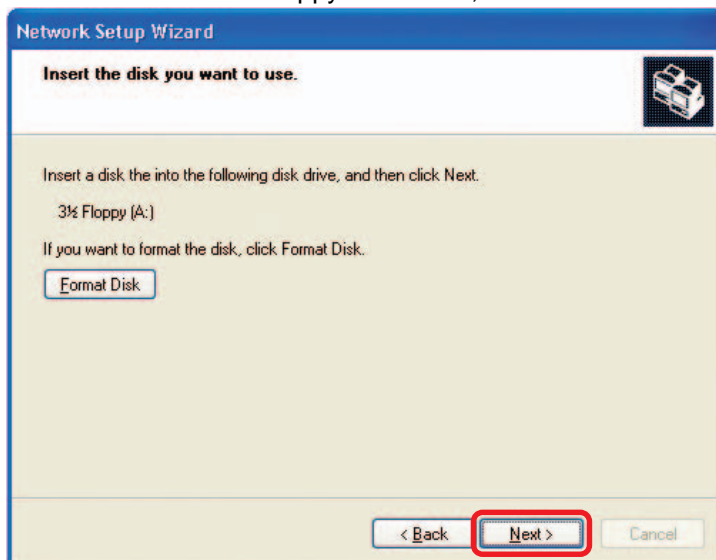
Networking Basics (continued)
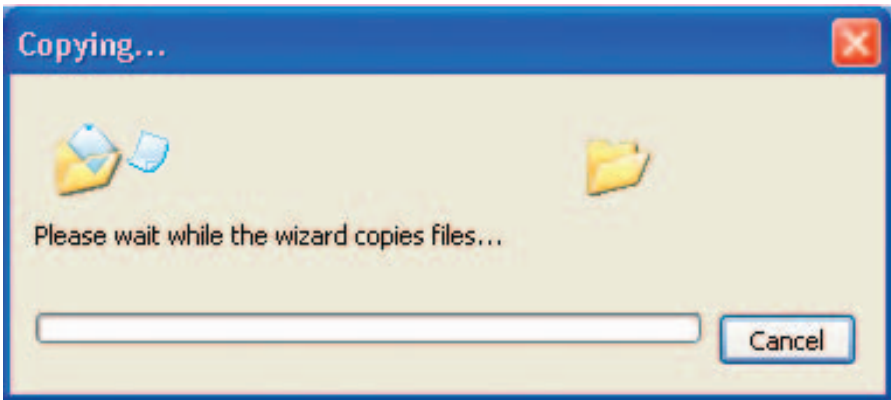
Please read the information under **Here's how** in the screen below. After you complete the **Network Setup Wizard** you will use the **Network Setup Disk** to run the **Network Setup Wizard** once on each of the computers on your network. Click **Next.**
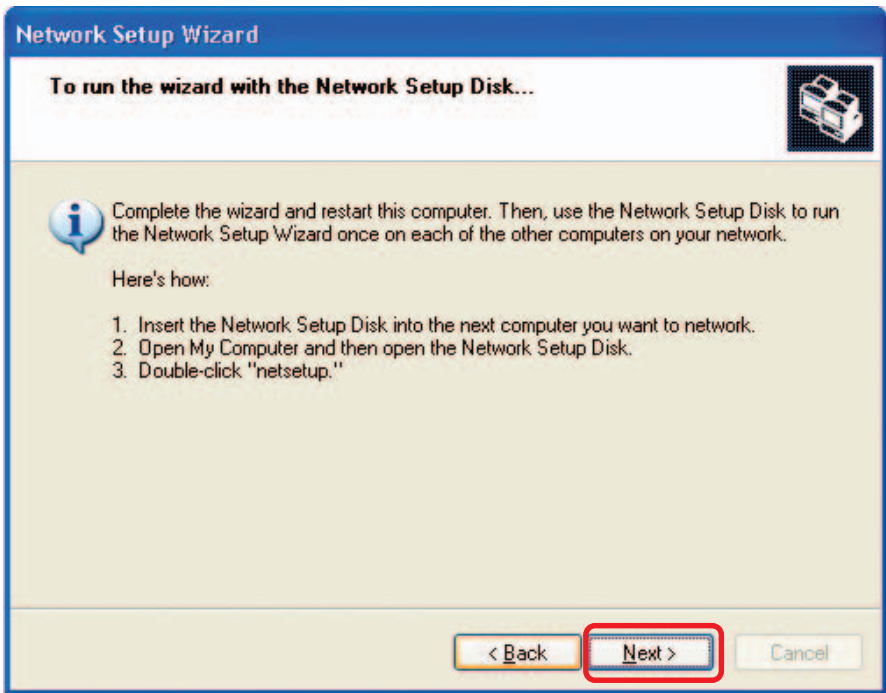
Networking Basics (continued)

Please read the information on this screen, then click **Finish** to complete the **Network Setup Wizard**.
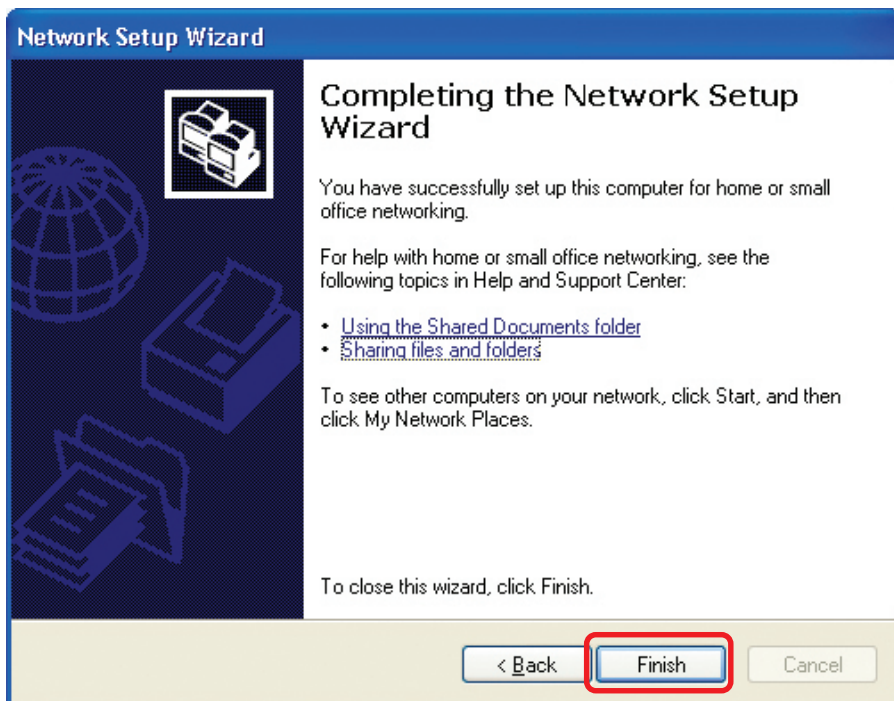
The new settings will take effect when you restart the computer. Click **Yes** to restart the computer.
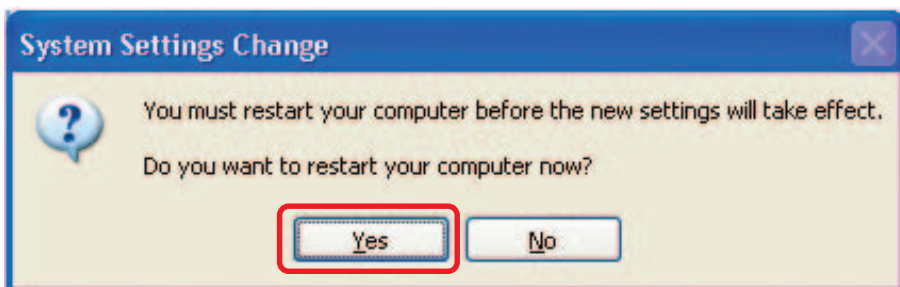
You have completed configuring this computer. Next, you will need to run the **Network Setup Disk** on all the other computers on your network. After running the **Network Setup Disk** on all your computers, your new Windows network will be ready to use.

Networking Basics (continued)

Naming your Computer

To name your computer In **Windows XP**, please follow these directions:

- Click **Start** (in the lower left corner of the screen).

- **Right-click** on **My Computer.**

- Select **Properties.**

- Select the **Computer Name Tab** in the System Properties window.

- You may enter a **Computer Description** if you wish; this field is optional.

- To rename the computer and join a domain, click **Change**.
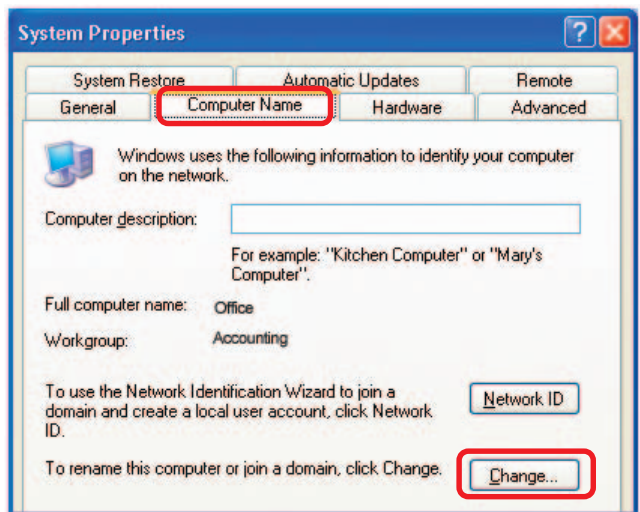
Networking Basics (continued)

Naming your Computer (continued)

- ■ In this window, enter the **Computer name**.

- ■ Select **Workgroup** and enter the name of the **Workgroup**.

- ■ All computers on your network must have the same **Workgroup** name.

- ■ Click **OK.**
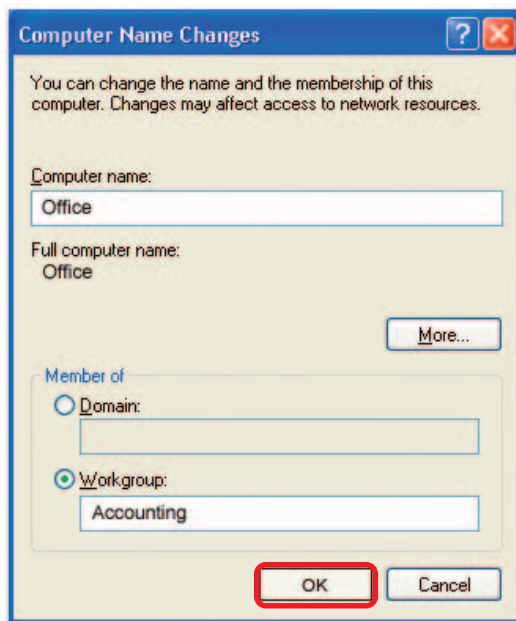
Checking the IP Address in Windows XP

The adapter-equipped computers in your network must be in the same IP Address range (see *Getting Started* in this manual for a definition of IP Address Range.) To check on the IP Address of the adapter, please do the following:

- ■ Right-click on the *Local Area Connection icon* in the task bar.

- ■ Click on **Status.**
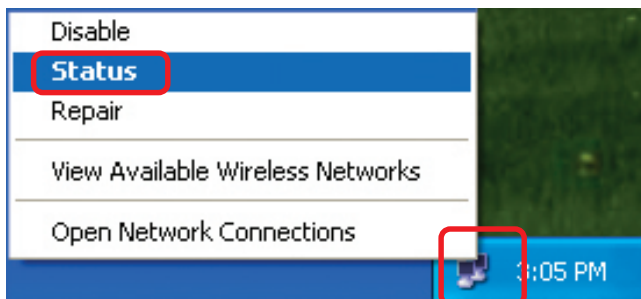
Networking Basics (continued)

Checking the IP Address in Windows XP (continued)

This window will appear.

■ Click the **Support tab.**

■ Click **Close.**
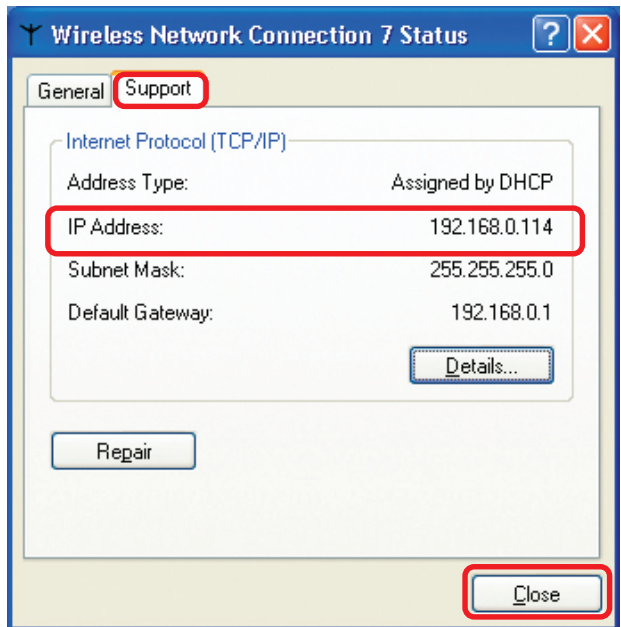
Assigning a Static IP Address in Windows XP/2000

Note: Residential Gateways/Broadband Routers will automatically assign IP Addresses to the computers on the network, using DHCP (Dynamic Host Configuration Protocol) technology. If you are using a DHCP-capable Gateway/Router you will not need to assign Static IP Addresses.

If you are not using a DHCP capable Gateway/Router, or you need to assign a Static IP Address, please follow these instructions:

■ Go to **Start.**

■ Double-click on **Control Panel.**
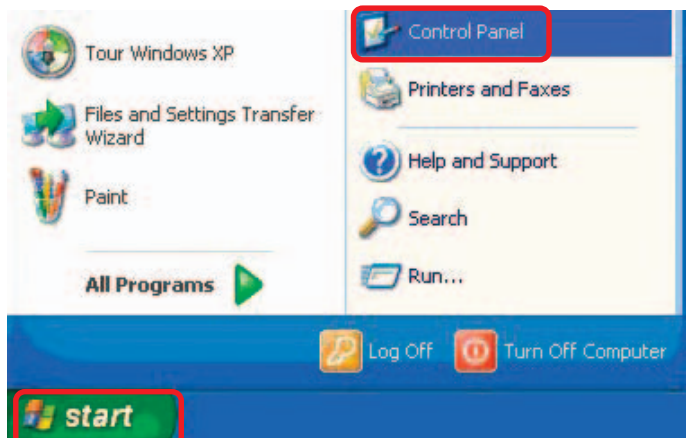
Networking Basics (continued)

Assigning a Static IP Address in Windows XP/2000 (continued)

■ Double-click on **Network Connections.**
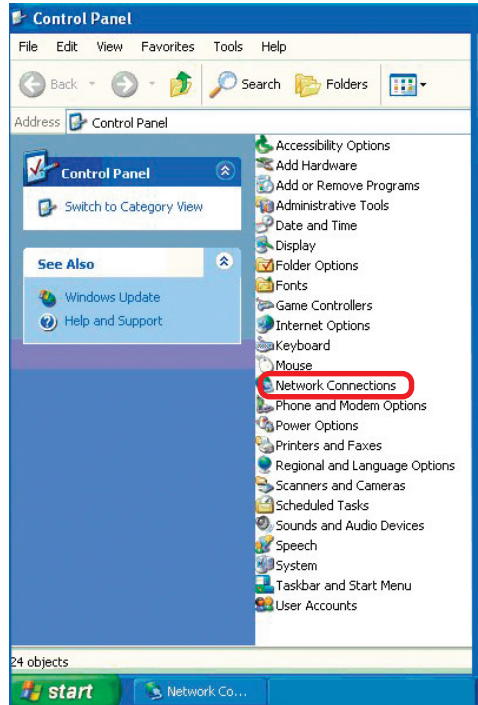
■ Right-click on **Local Area Connections.**

■ Double-click on **Properties.**
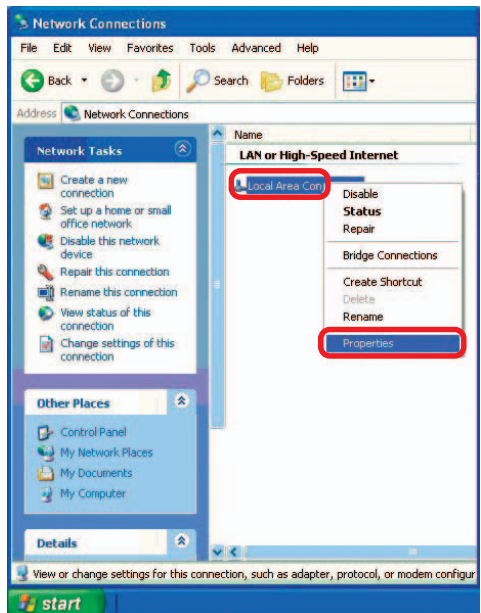
Networking Basics (continued)

Assigning a Static IP Address in <u>Windows XP/2000</u>

■ Click on **Internet Protocol (TCP/IP).**

■ Click **Properties.**

■ Input your **IP Address and subnet mask.** (The IP Addresses on your network must be within the same range. For example, if one computer has an IP Address of 192.168.0.2, the other computers should have IP Addresses that are sequential, like 192.168.0.3 and 192.168.0.4. The subnet mask must be the same for all the computers on the network).
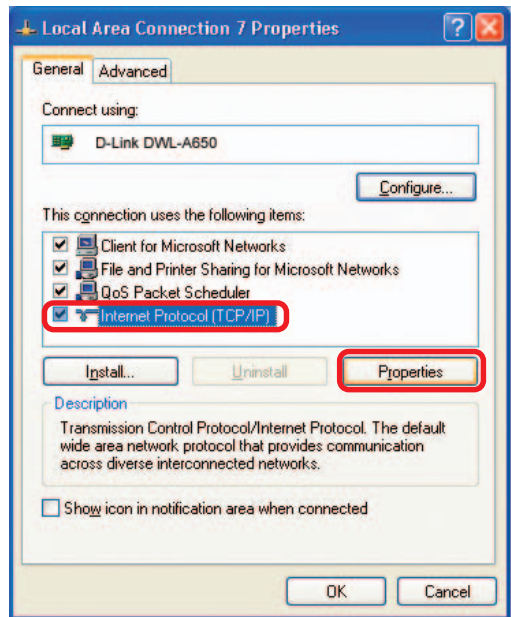
■ Input your **DNS server addresses.** **Note: If you are entering a DNS server, you must enter the IP address of the Default Gateway (the IP address of the firewall).**

The DNS server information will be supplied by your ISP (Internet Service Provider.)

■ Click **OK.**
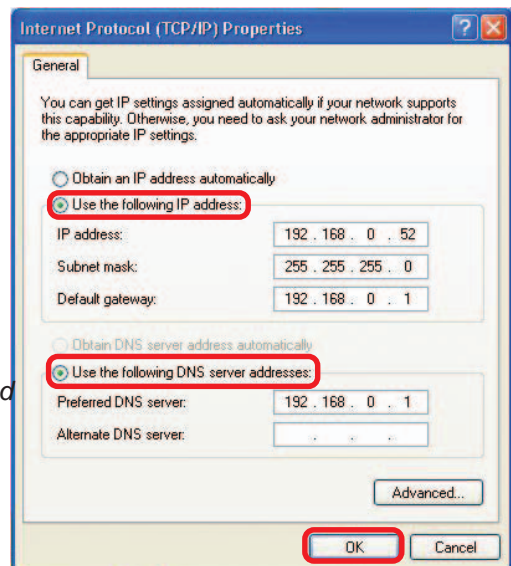
Networking Basics (continued)

Assigning a Static IP Address with Macintosh OSX

■ Go to the **Apple Menu** and se-
lect **System Preferences.**

■ Click on **Network.**
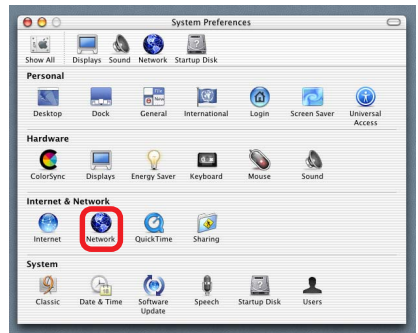
■ Select **Built-in Ethernet** in the
Show pull-down menu.

■ Select **Manually** in the
Configure pull-down
menu.
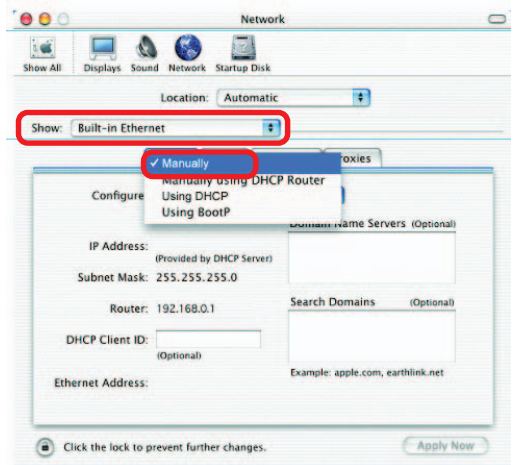
■ Input the **Static IP Address**,
the **Subnet Mask** and the
Router IP Address in the
appropriate fields.

■ Click **Apply Now.**

75

Networking Basics (continued)

Selecting a Dynamic IP Address with <u>Macintosh OSX</u>

- Go to the **Apple Menu** and select **System Preferences.**

- Click on **Network.**

- Select **Built-in Ethernet** in the **Show** pull-down menu.
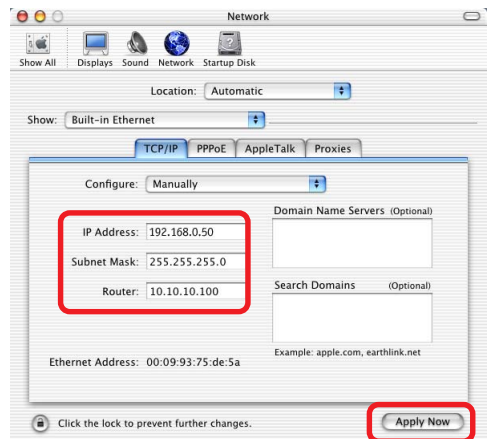
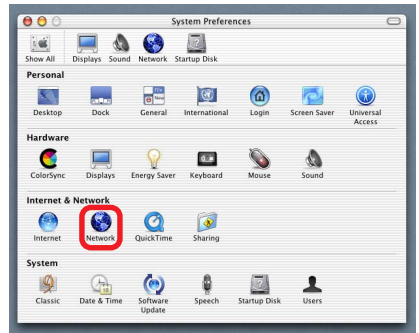- Select **Using DHCP** in the **Configure** pull-down menu.
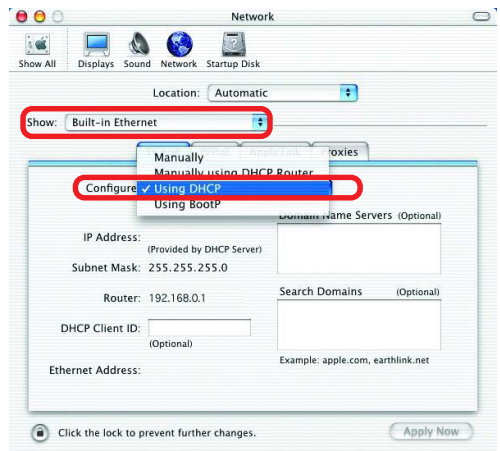
- Click **Apply Now.**

- The **IP Address, Subnet mask**, and the **Router's IP Address** will appear in a few seconds.
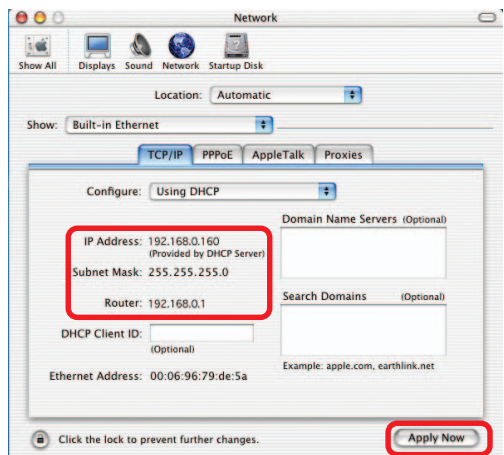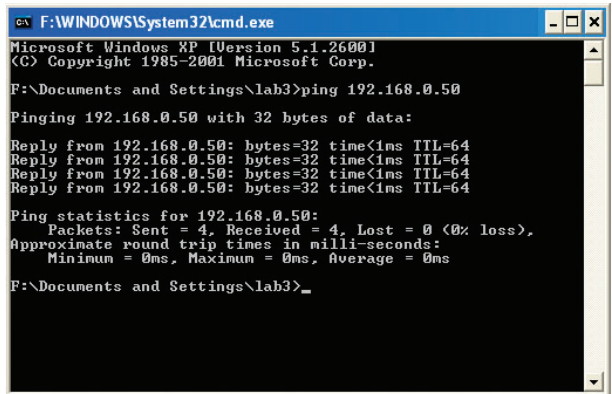
Networking Basics (continued)

Checking the Wireless Connection by Pinging in Windows XP/2000

Note: The following illustrations are examples only. The IP Address that you are pinging may be different from those in the following examples.

■ Go to **Start** > **Run** > type **cmd**. A window similar to this one will appear. Type **ping xxx.xxx.xxx.xxx**, where **xxx** is the **IP Address** of the Wireless Router or Access Point. A good wireless connection will show four replies from the Wireless Router or Acess Point, as shown.
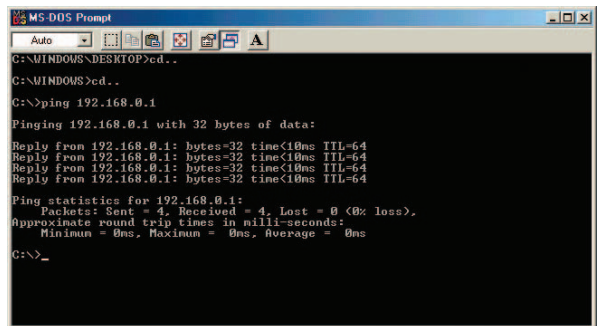
Checking the Wireless Connection by Pinging in Windows Me/ 98SE

■ Go to **Start** > **Run** > type **command**. A window similar to this will appear. Type **ping xxx.xxx.xxx.xxx** where **xxx** is the **IP Address** of the Wireless Router or Access Point. A good wireless connection will show four replies from the wireless router or access point, as shown.

Technical Specifications

Functions Provided

4 10/100Mbps Fast Ethernet ports for dual WAN connection, trusted LAN connection and untrusted LAN connection

Manages up to 250 user accounts via the internal user account database

ID/Password based authentication and authorization- Can be combined with MAC Address locking to provide stricter access control

POP3, RADIUS and LDAP external authentication mechanism support - Only one of these can be selected at a time

On-line status monitoring and history traffic data review

SSL protected access to the administration interface and user authentication interface

Customizable user login, logout web interface

Customizable target URL for users who successfullly get authorization

Built-in DHCP server

High-speed policy routing engine

Customizable peremptory traffic redirection NTP client

Local network port for connecting a trusted network

Permits access to WAN and LAN from local network without authentication

Permits connection to wired Ethernet while connecting the wireless network to this Ethernet port

Technical Specifications (continued)

Device Ports

WAN1 port: 10/100Mbps Fast Ethernet

WAN2 port: 10/100Mbps Fast Ethernet

Private LAN port: 10/100Mbps Fast Ethernet connects to workstations & servers that do not need authentication

Public LAN port: 10/100Mbps Fast Ethernet connects to workstations & devices that need authentication

Console port: RS-232 (default set to 115200, n, 8, 1, no flow control)

Power Supply

PC Power Cord

Power Input

110 VAC

Operating Temperature

0° - 50°C

Storage Temperature

-25° - 55°C

EMI Certification

FCC Class A
CE Class A
VCCI Class A
C-Tick

Safety

UL
CSA
TUV/GS
T-Mark

Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers within the United States and within Canada for the duration of the warranty period on this product.

U.S. and Canadian customers can contact D-Link technical support through our web site, or by phone.

Tech Support for customers within the United States:

D-Link Technical Support over the Telephone:
(877) 453-5465
Twenty four hours a day, seven days a week.

D-Link Technical Support over the Internet:
http://support.dlink.com
email:support@dlink.com

Tech Support for customers within Canada:

D-Link Technical Support over the Telephone:
(800) 361-5265
Monday through Friday 7:30am to 12:00am EST

D-Link Technical Support over the Internet:
http://support.dlink.ca
email:support@dlink.ca

D-Link

Limited Warranty   (USA only)

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited warranty for its product only to the person or entity that originally purchased the product from:

- D-Link or its authorized reseller or distributor and
- Products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link products described below will be free from material defects in workmanship and materials from the date of original retail purchase of the product, for the period set forth below applicable to the product type ("Warranty Period"), except as otherwise stated herein.

1-Year Limited Warranty for the Product(s) is defined as follows:

- Hardware (excluding power supplies and fans) One (1) Year
- Power Supplies and Fans One (1) Year
- Spare parts and spare kits Ninety (90) days

D-Link's sole obligation shall be to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund at D-Link's sole discretion. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or have an identical make, model or part. D-Link may in its sole discretion replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement Hardware will be warranted for the remainder of the original Warranty Period from the date of original retail purchase. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link's sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund at D-Link's sole discretion. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Software will be warranted for the remainder of the original Warranty Period from the date or original retail purchase. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for hardware and software of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.

- The original product owner must obtain a Return Material Authorization ("RMA") number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the Product and will not ship back any accessories.

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708**. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer and upon request.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered: This limited warranty provided by D-Link does not cover: Products, if in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. Repair by anyone other than D-Link or an Authorized D-Link Service Office will void this Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY

04/18/06

Appendix
Windows TCP/IP Setup

If you have not changed the factory default settings of the DSA-5100 in Windows XP/ 2000/ME/98SE TCP/IP, it is not necessary to make any modification here. With the factory default settings, the DSA-5100 will automatically assign an appropriate IP address (and related information) to each PC after the PC has been booted.

You can check the TCP/IP setup according to the following procedure:

Check the TCP/IP Setup of Windows ME/98SE
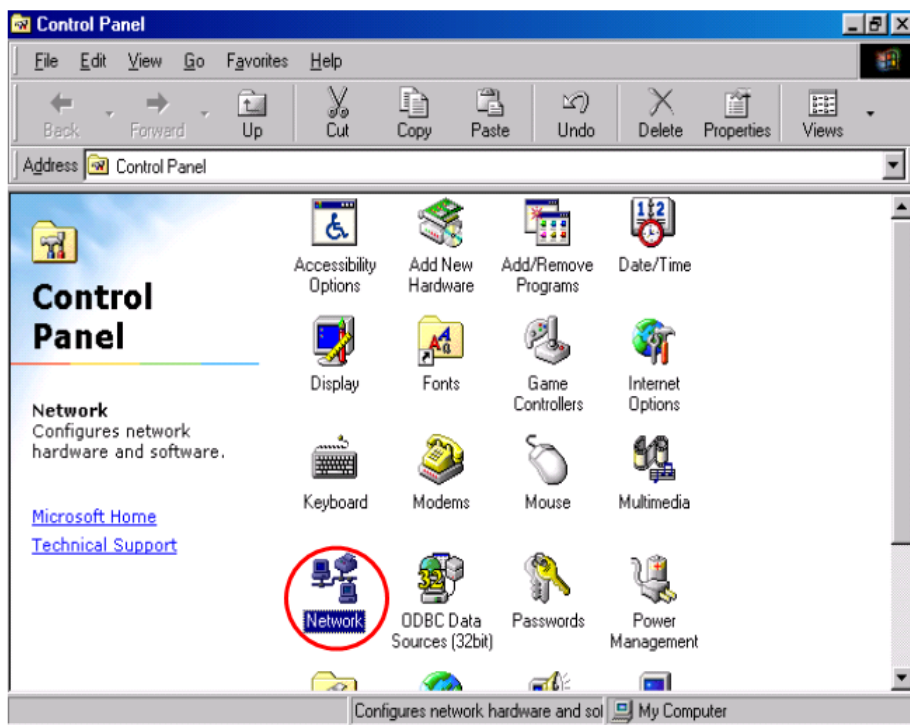
Select **Start** > **Control Panel** > **Network**

Appendix
Windows TCP/IP Setup
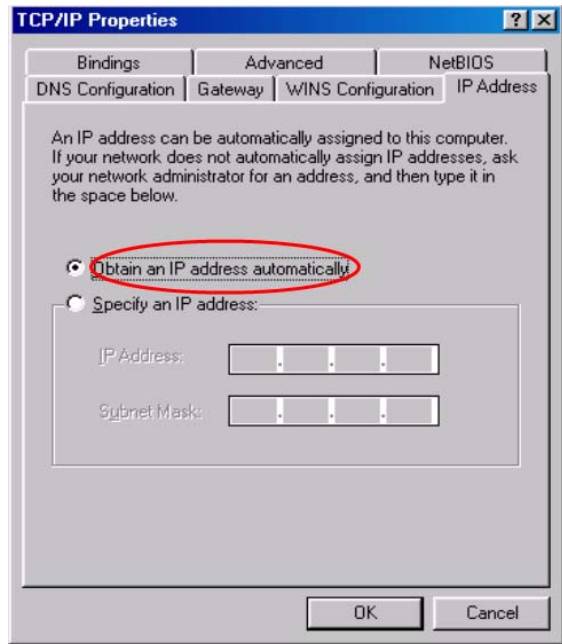### Check the TCP/IP Setup of Windows ME/98SE (continued)

Select the TCP/IP communication protocol of the network card.

Click **Properties**.
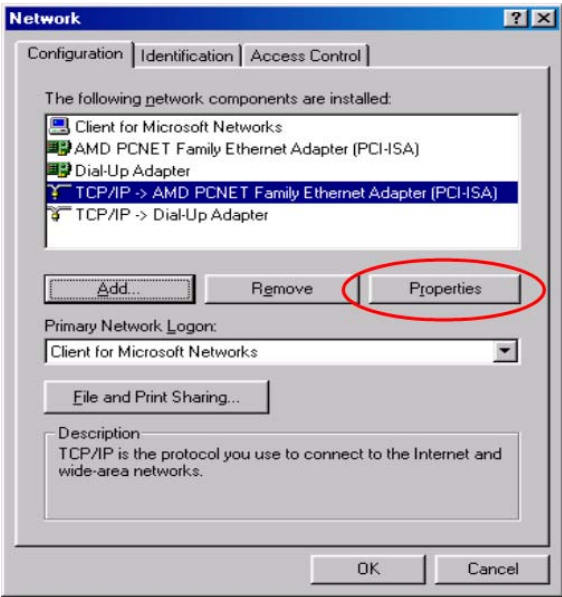
Using DHCP

If you want to use DHCP, please select **Obtain an IP Address Automatically**, which is also the default setting of Windows. Reboot the PC to make sure an IP address is obtained from the DSA-5100.

Appendix

Windows TCP/IP Setup
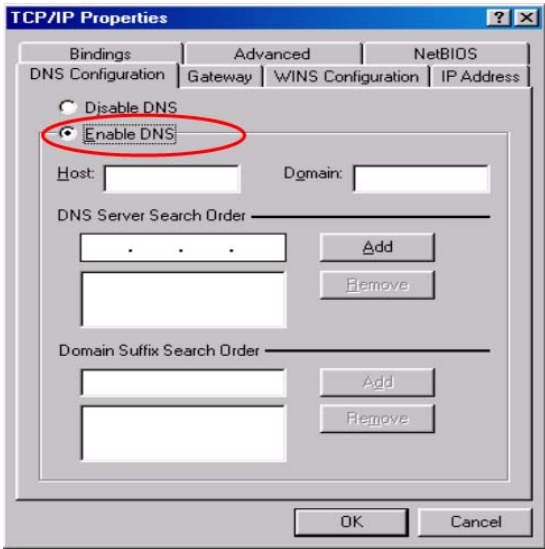
Check the TCP/IP Setup of Windows ME/98SE (continued)

Using a Specific IP Address
If you have completed the setup for your PC, please inform the network administrator before modifying the following setup.

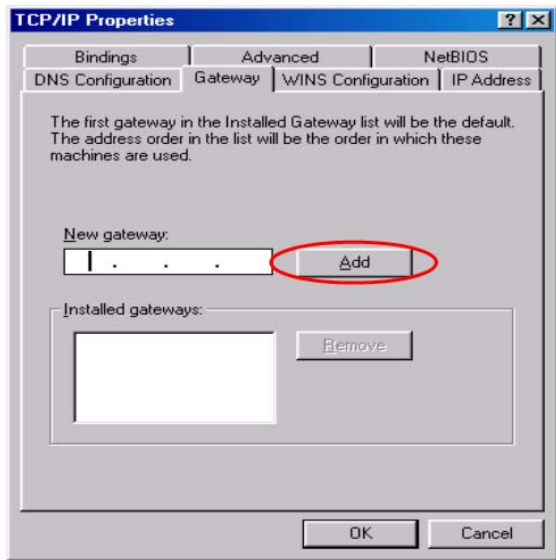If the DNS Server column is blank, please click **Enable DNS**.

Enter the DNS address or the DNS address provided by your ISP.

Click **OK**.

Select the **Gateway** tab, and enter the IP address of the DSA-5100.

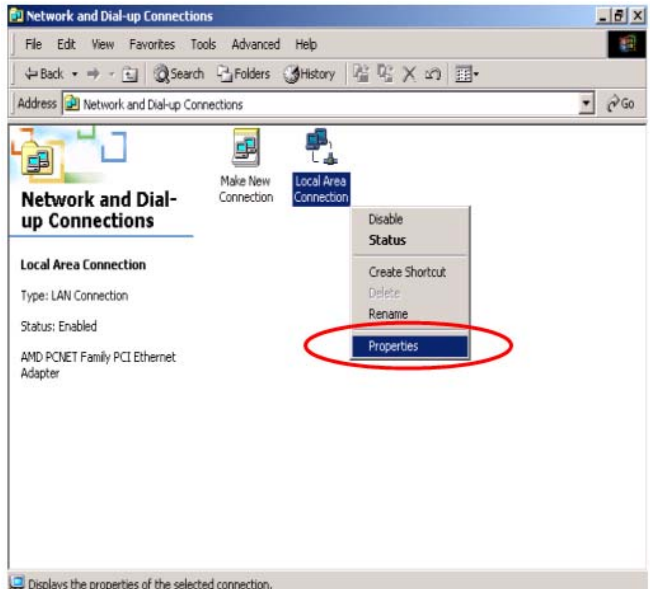Click **Add**.

Appendix

Windows TCP/IP Setup

Check the TCP/IP Setup of Windows 2000

Select **Start**>
Control Panel>
**Network and
Dial-up Connections**

Right-click
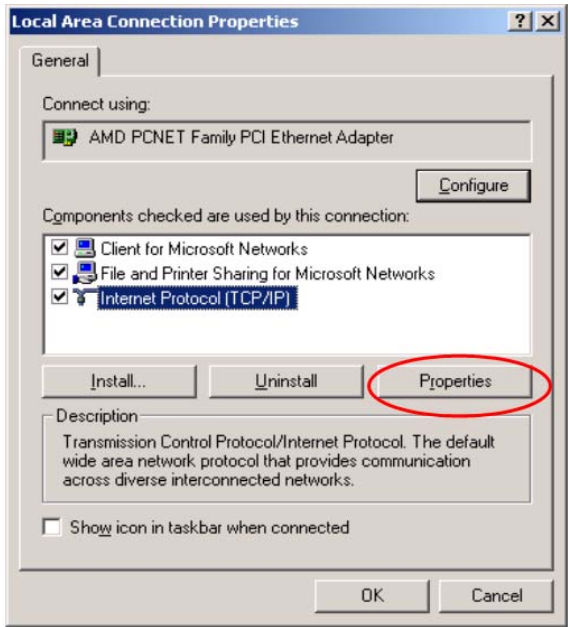**Local Area Connection.**

Select **Properties.**

Appendix

Windows TCP/IP Setup

Check the TCP/IP Setup of Windows 2000 (continued)

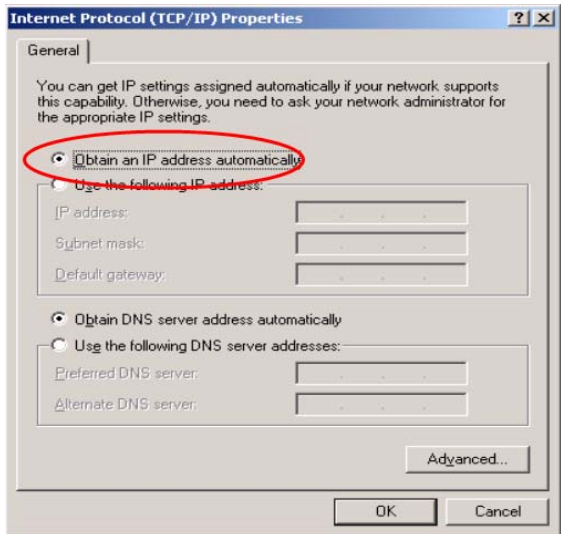Select Internet Protocol(TCP/IP).

Click **Properties**.

Using DHCP

If you want to use DHCP, please select **Obtain an IP Address Automatically**, which is also the default setting.

Reboot the PC to make sure an IP address is obtained from the DSA-5100.
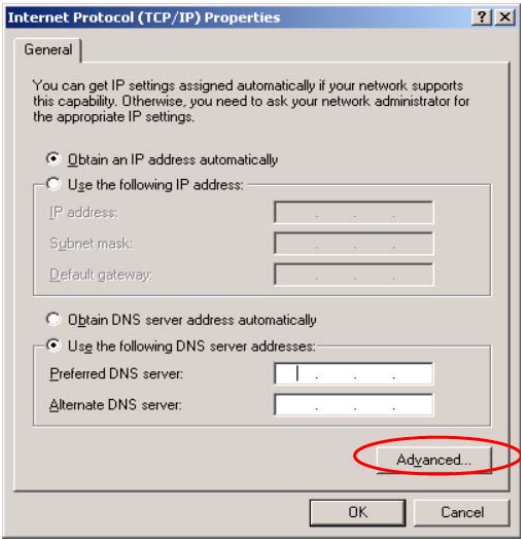
Appendix

Windows TCP/IP Setup

Check the TCP/IP Setup of Windows 2000 (continued)

Using a Static IP Address

If you have completed the setup for your PC, please inform the network administrator before modifying the following setup.
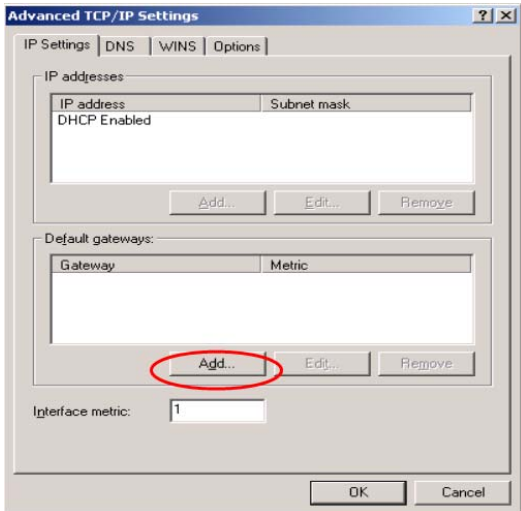
Click **Advanced** in the TCP/IP properties.

Select the **IP Settings** tab.

Click **Add.**

Enter the IP address of the DSA-5100 in the **Default Gateways** column.

Click **Add**.

Appendix

Windows TCP/IP Setup

Check the TCP/IP Setup of Windows 2000 (continued)

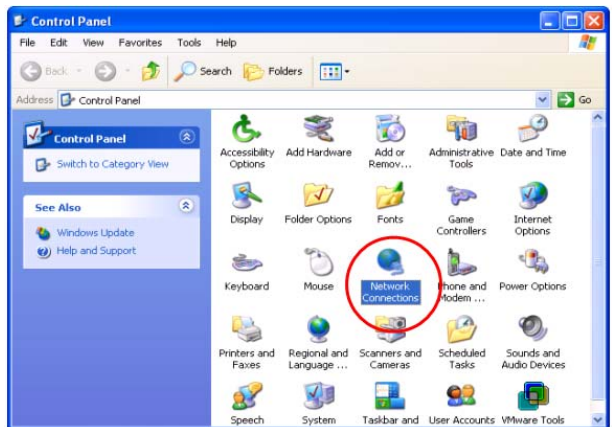Click **Using the following DNS Server Address**.

Enter the DNS address provided by your ISP.

Click **OK**.

Check the TCP/IP Setup of Windows XP

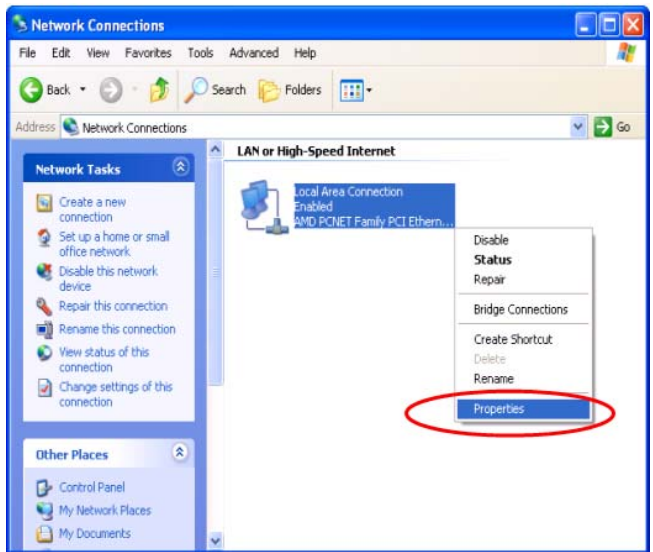Select **Start** > **Control Panel** > **Network Connection**.

Appendix

Windows TCP/IP Setup

Check the TCP/IP Setup of Windows XP (continued)
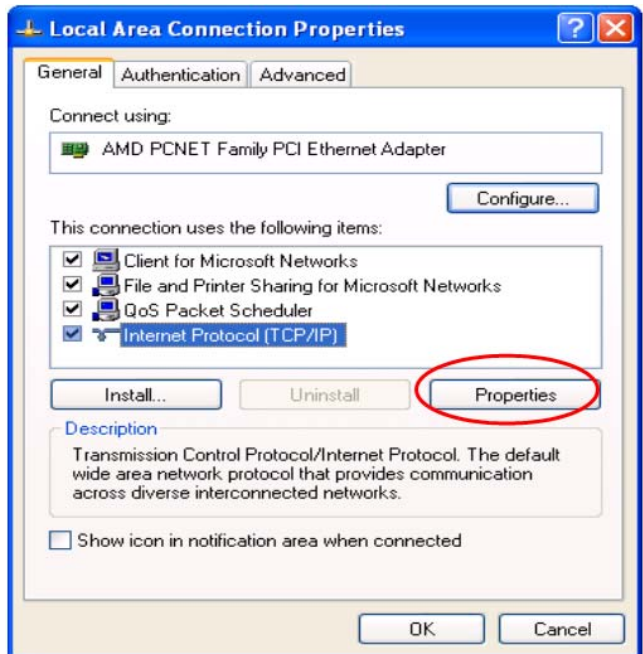
Right-click
Local Area Connection.

Select **Properties**.

Select the **General** tab.

Select
**Internet Protocol
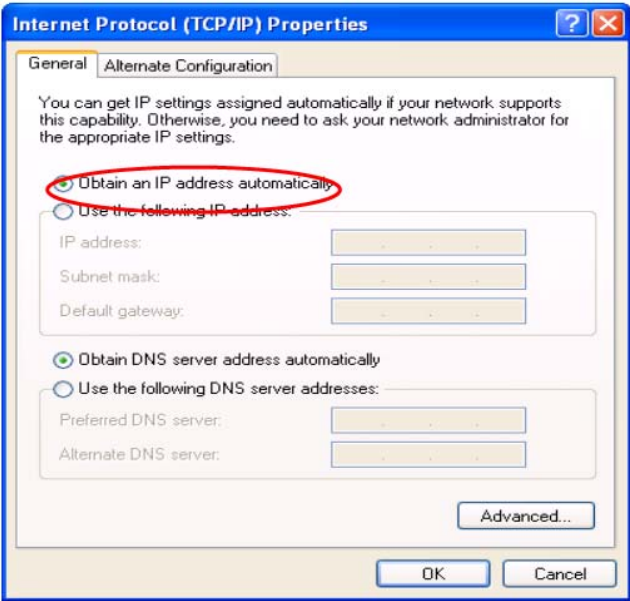(TCP/IP)**.

Click **Properties.**
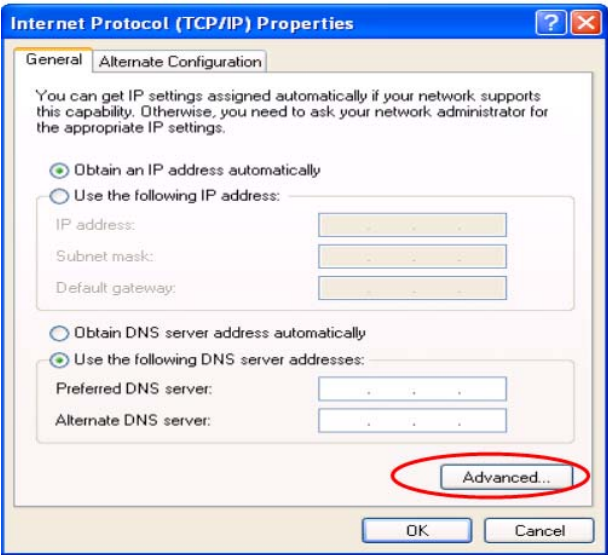
Appendix

Windows TCP/IP Setup

Check the TCP/IP Setup of Windows XP (continued)

If you want to use DHCP, please select **Obtain an IP Address Automatically**.

Click **OK**.

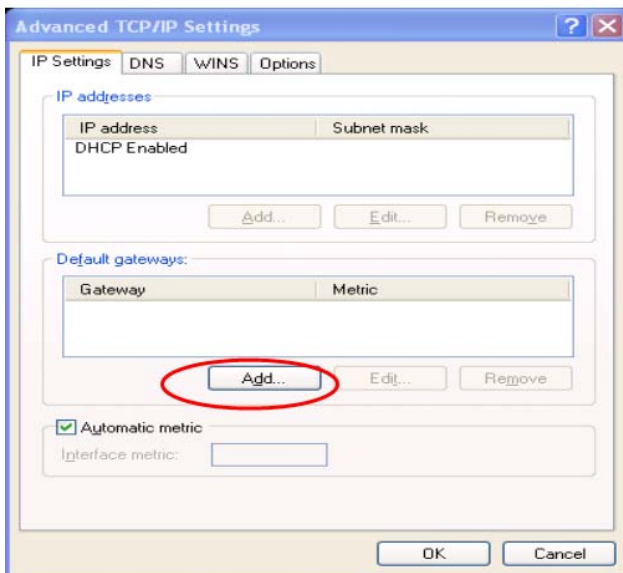**Using the Static IP Address**

Click **Advanced**.

Appendix

Windows TCP/IP Setup
Check the TCP/IP Setup
in Windows XP

Click the **IP Settings** tab.

Enter the IP address of the DSA-5100 in the **Default Gateways** column.

Click **Add**.

Click **OK**.

If the DNS Server field is blank, select **Use the following DNS Server Addresses**.

Enter the DNS address.

Click **OK**.